PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6:
G06F 17/60

A1

(11) International Publication Number: WO 00/25245

(43) International Publication Date: 4 May 2000 (04.05.00)

(21) International Application Number: PCT/US99/24570

(22) International Filing Date: 20 October 1999 (20.10.99)

(30) Priority Data:
60/105,778 27 October 1998 (27.10.98) US
09/223,691 30 December 1998 (30.12.98) US

(71) Applicant: RECEIPT.COM, INC. [US/US]; 440 Clyde Avenue, Mountain View, CA 94043 (US).

(72) Inventor: JEVANS, David; 17755 Big Basin Highway, Boulder Creek, CA 94043 (US).

(74) Agent: WOLFELD, Warren, S.; Fliesler Dubb Meyer & Lovejoy LLP, Four Embarcadero Center, Suite 400, San Francisco, CA 94111-4156 (US).

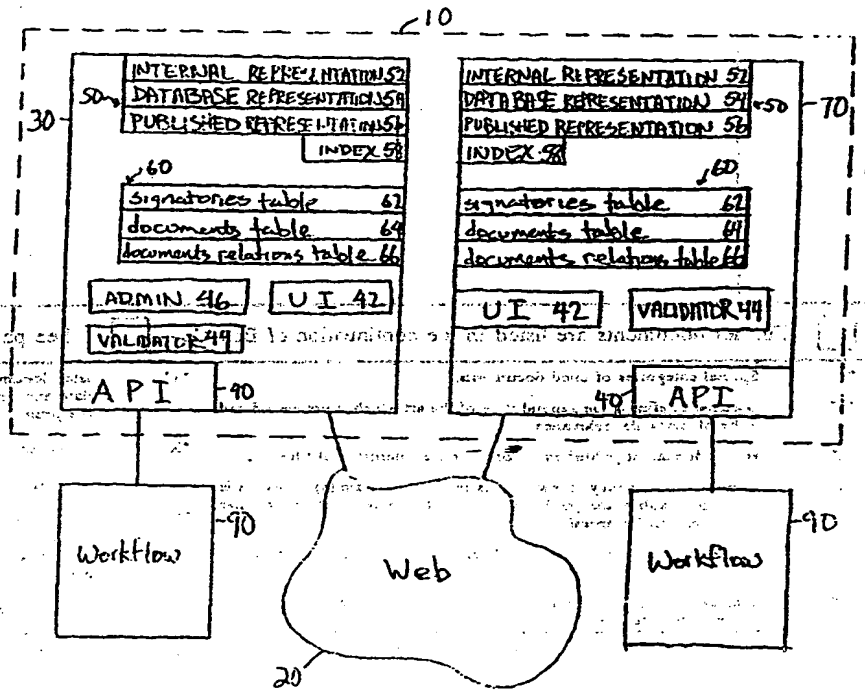
(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: MECHANISM FOR MULTIPLE PARTY NOTARIZATION OF ELECTRONIC TRANSACTIONS

(57) Abstract

A method and apparatus for conducting electronic transactions and auditing electronic transaction documents in an online transaction system allow users to accept or reject received electronic transaction documents, wherein the acceptance is non-repudiable and is based on the content and terms of the received electronic transaction document. Transactions may be conducted between two or more parties, and may include non-party participants. Electronic transaction documents may be stored and audited by validating digital signatures and verifying that the contents of stored electronic transaction documents have not been compromised.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania
AM	Armenia
AT	Austria
AU	Australia
AZ	Azerbaijan
BA	Bosnia and Herzegovina
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CU	Cuba
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GH	Ghana
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IL	Israel
IS	Iceland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgyzstan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakstan
LC	Saint Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho
LT	Lithuania
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
MK	The former Yugoslav Republic of Macedonia
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
MX	Mexico
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SN	Senegal
SZ	Swaziland
TD	Chad
TG	Togo
TJ	Tajikistan
TM	Turkmenistan
TR	Turkey
TT	Trinidad and Tobago
UA	Ukraine
UG	Uganda
US	United States of America
UZ	Uzbekistan
VN	Viet Nam
YU	Yugoslavia
ZW	Zimbabwe

MECHANISM FOR MULTIPLE PARTY NOTARIZATION OF ELECTRONIC TRANSACTIONS

This application claims priority of U.S. provisional patent application Serial Number 60/105,778, filed October 27, 1998, which is co-pending and incorporated by reference herein.

FIELD OF THE INVENTION

The invention relates to computer systems used for business transactions, and more particularly to client-server software systems which exchange business transaction data between participants to business transactions.

BACKGROUND OF THE INVENTION

When companies engage in commerce activities using computers, software systems are employed that handle all manner of business management and communications. The operation of these systems results in the execution of business transactions. Business management systems include accounting, order processing, job tracking, billing and resource planning. Business communications systems include electronic mail (e-mail) for exchanging messages between people, electronic data interchange (EDI) for sending and receiving structured messages for purchasing, inventory control and financial payments between organizations. In recent years World Wide Web (referred to herein as the "Web") technology has allowed companies to provide interfaces to business systems, workflow and collaboration through standardized Web browsers such as Microsoft Internet Explorer, Netscape Navigator and Netscape Communicator. All of these systems can allow some form of commercially significant business transaction. Companies need to track, manage, verify, audit and share records of these business transactions.

Electronic commerce systems have traditionally been based on EDI technologies, where companies exchange highly structured messages that conform

to ANSI or ISO standards for describing a myriad of product ordering, tracking and payments. EDI messages are typically generated from a company's order processing or requisition system and sent to a communications system that transmits the message over a computer network to the destination company. When an EDI message is delivered from one company to another, the message is loaded into a data conversion system that will convert the standardized EDI message data format into the data format required by the receiving company's order processing system.

Many electronic commerce systems incorporate cryptographic functions at the level of the communications subsystem. For example, a communications subsystem (which might be an e-mail system, for example), might automatically add a digital signature to each message transmitted from one party to another, to enable the recipient's communications subsystem to verify the authenticity of the message. But these functions take place at the level of the communications subsystem, not at the level of the order processing or requisition system. They are frequently transparent to the order processing or requisition system, and to the users. The digital signature appended to the message might be that of the company instead of the individual who placed or acknowledged an order, and no auditable record is kept in the order processing or requisition system of who signed each message sent or received. Many electronic commerce systems also return an acknowledgment to a message sender that a message was received. But again, such acknowledgments often occur automatically at the level of the communication subsystem and are often transparent to the order processing or requisition systems and users. They evidence only safe receipt of a message, not acceptance of anything contained in the message (such as terms and conditions of a transaction). Some electronic commerce systems do provide electronic acknowledgments originating at the level of the order processing or requisition, but these are often not digitally signed (except perhaps by the communication subsystem, with all its attendant problems), and certainly are not intended to evidence legally binding acceptance of the message content.

New forms of electronic commerce are available using Web technologies. These systems allow many users to access an online catalog. Customers can browse the catalog with a standard Web browser and can order products using this interface. When a product is ordered, many of these servers will print an order tracking number on the screen so that the customer has some reference to the order in case the customer has a problem or question regarding the delivery of the product or service that was purchased. Some systems will send an e-mail message to the customer, and the e-mail message will contain the order number in it.

A number of financial services companies, particularly banks and stock brokers, use similar technology to enable customers to access bank and stock accounts and to make monetary transfers, bill payments or perform stock trades over the Web. Like electronic catalog commerce systems, these financial services systems might print an order tracking number to the screen or may send an e-mail message containing the order tracking number. Some providers also send a printed paper receipt to the customer using regular postal service.

Another type of business transaction involves the acceptance of terms and conditions and contracts online. Typically an online service that is offered over a Web browser or with custom software (for example a home banking application with customized software on the client computer that communicates to a server at the bank over a computer network) prints a screen of contractual terms regarding the use of the service. The customer is asked to click a button that concerns the customer's acceptance of these terms and conditions. Once a customer accepts these terms, the service is activated. The service provider can legally cancel the service agreement if the customer violates these terms. Some of these services send an e-mail message that recapitulates the terms and conditions that were accepted by the customer. However, the majority of these services provide absolutely no record to the customer of the terms and conditions, and likewise provide very little in the way of proof that the customer actually accepted these terms.

A similar situation to the terms and conditions of online services exists in the acceptance of software license agreements. Typically a software program presents a license agreement to the customer when the software is installed or used for the first time. When the customer clicks a button to signify agreement to these terms, the software becomes operational. Usually there is no mechanism for the customer to save these terms and conditions for later review or for approval by an attorney prior to signifying agreement.

Many companies use collaboration and groupware tools such as Lotus Notes or Web-based systems to share information and business documents within the company and sometimes with business partners or customers. These systems sometimes provide a form of centralized tracking and auditing of the actions that people have taken in the system. Usually this consists of log files which are text files that contain an ever growing list of actions that the software performed, usually in human-readable format. Another mechanism is provided by such systems allows activity to be recorded in an application-specific database.

When companies use electronic mail (e-mail) to exchange messages and files with employees, customers or partners, there is often no way to verify that the message was received and read by the intended recipient. Some systems ask for the receiver to send an e-mail that confirms the receipt of the message. Other systems (see Tumbleweed U.S. Patent No. 5,790,790, incorporated herein by reference) use a database and Web based system to track when the message was received. The message to be sent is stored in a database on a server. An e-mail message is sent to notify the recipient that a message was sent and instructing the recipient to visit a Web site to retrieve the message. The Web site is an interface to the message store database. When the recipient uses a Web browser to view the message on the Web server, the underlying database makes a record that the message was viewed. With these systems the sender can use a Web-based interface to see if and when the user has read the message.

Finally, in U.S. Patent No. 5,739,512 (incorporated by reference herein), a mechanism is described whereby a consumer purchase made at a cash register with a credit card or smart card can generate a digital receipt that is e-mailed to the e-mail address of the purchaser. The intent of the '512 system is to provide the purchaser with an electronic record of the purchase. Such a record could presumably be used by the purchaser to be entered into an accounting or expense tracking system to track his or her purchases for reimbursement by an employer.

Thus, there is a need for an online transaction system that allows users to conduct online transactions in a manner that evidences a participant's acceptance of the transaction.

SUMMARY OF THE INVENTION

According to the invention, roughly stated, an online transaction system allows users to accept or reject received electronic transaction documents, wherein the acceptance is non-repudiable and is based on the content and terms of the received electronic transaction document.

In one aspect, the present invention provides a method and apparatus for conducting electronic transactions between at least first and second parties in which the first party sends to the second party an electronic transaction document evidencing content which is non-repudiable by the first party; the second party may accept the content of the electronic transaction document and send a response to the first party that is non-repudiable by the second party.

In another aspect, the present invention provides a method and apparatus for conducting electronic transactions between at least first and second parties in which the first party obtains the digital signature of a non-party participant and includes this in an electronic transaction document evidencing content that is non-repudiable by the first party; the first party transmits the electronic document to a second party; the second party may accept the content of the electronic transaction document and send a response to the first party that is non-repudiable by the second

party. The second party may also obtain the digital signature of another non-party participant and include this in the non-repudiable response.

In yet another aspect, the present invention provides a method and apparatus for auditing electronic transaction documents by validating digital signatures and verifying that the content of stored electronic transaction documents has not been compromised.

Other features and benefits of the present invention will be apparent from the detailed description of the invention when considered with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be described with respect to particular embodiments thereof, and reference will be made to the drawings in which:

Fig. 1 illustrates symbolically the architecture of the which may be used for implementing the present invention;

Fig. 2 illustrates symbolically the electronic transaction document;

Figure 3 is a flowchart showing the steps which are performed to conduct an online transaction;

Fig. 4 is a flowchart showing the steps which are performed to reject an electronic transaction document;

Fig. 5a is a flowchart showing the steps which are performed to gather multiple digital signatures in parallel;

Fig. 5b is a flowchart showing the steps which are performed to gather multiple digital signatures in a serial manner;

Fig. 6a is a flowchart showing the steps which are performed to conduct a transaction requiring the digital signature of a single non-party participant;

Fig. 6b is a flow diagram showing the logical sequence of steps executed by the present invention to conduct a transaction requiring the digital signatures of multiple non-party participants;

Fig. 7a is an illustration of a user interface screen used to view and accept electronic transaction documents;

Fig. 7b is an illustration of a user interface screen used to display and manipulate received electronic documents;

Fig. 7c is an illustration of a user interface screen showing a list of related documents;

Fig. 7d is flowchart showing the steps which are performed to audit electronic transaction documents; and

Fig. 8 is a schematic in block diagram form showing a high level representation of a computer system used to implement the present invention.

DETAILED DESCRIPTION

A transaction is a communicative action or activity involving two or more parties that reciprocally affect or influence each other. Important examples of transactions include promises and agreements which describe current or future activity or inactivity, as well as activities that have already taken place. As used herein, the term "transaction" includes sub-transactions, which are transactions that are themselves parts of larger transactions. For example, a transaction that is an agreement includes a transaction in which one party makes a promise to a second party, and another transaction in which the second party makes a promise to the first party. As another example, an agreement among three parties may include one transaction in which party A makes promises to party B, and a second transaction in which party B makes promises to party C, and so on.

Entities participating in transactions may include party and non-party participants. "Parties" are the primary participants in a transaction, and indicate consent to be bound to the terms of the transaction by attaching signatures to the document evidencing the transaction. If the transaction includes a promise, for example, the party participants in the transaction include the promisor and the promisee. Non-party participants include entities such as notaries, auditors, or other

signatories required to serve to validate the transaction, grant permission to a party to participate in a transaction, or otherwise serve as a witness to the transaction. The signature of a non-party participant serves to acknowledge the transaction without incurring an obligation or indicating acceptance of terms by the non-party participant.

A promise can be conditional and/or one-sided. A purchase order, for example, can evidence a promise on the part of the purchaser to pay a certain amount of money if the vendor delivers the requested product or service. A credit card draft, for example, can evidence a promise on the part of the purchaser to pay money in accordance with a cardmember agreement. A credit card draft might also evidence activity that has already taken place, for example delivery of purchased goods from the vendor to the purchaser.

An "Agreement" includes reciprocal promises by or among at least two parties.

A transaction document describes the essence of a transaction. Transaction documents may include offer letters, purchase orders, acceptance letters, receipts, sales slips, etc. A transaction document is signed by or otherwise evidently associated with the party or parties incurring an obligation under that transaction document, and may also bear the signatures of non-party participants. Transaction documents establish that the transaction actually occurred, so that no party may later repudiate it. Transaction documents identify the terms of the transaction, the responsibilities of the respective parties to the transaction, any products, services or moneys exchanged, and bear non-repudiable marks of identification of the parties to the transaction, signifying their acceptance of the transaction. Transaction documents usually provide some safeguard that makes evident any alteration to the transaction document after a party has placed his or her non-repudiable mark on the transaction document. For example, carbon copies of transaction documents may be used to verify original transaction documents. As another example, signatures may be certified.

The basis of trust in transactions is the simultaneous presence of both parties to the agreement to witness the transaction document's content and signing. In the on-line world, such simultaneous presence is neither possible nor desirable. Instead, electronic transaction documents provide proof that copies held by both parties are identical with respect to terms and signatures. A transaction document sent from a first party to a second party often triggers a subsequent transaction document to be sent from the second party to the first party in response to the preceding transaction document.

As used herein, a given action or event occurs "in response to" to a preceding action or event if the preceding action or event influenced the given action or event. If there is an intervening action, event or time period, the given action or event can still be "in response to" the preceding action or event. If the intervening action, event or time period combines more than one action or event, the subsequent action or event is considered "responsive" to *each* of the action or event inputs. If the given action or event is the same as the preceding action or event, this is merely a degenerate case in which the given action or event is still considered to be "in response" to the preceding action or event.

The term "electronic transaction document" as used herein refers to an electronic document that establishes an online transaction between two or more participants. An electronic transaction document may contain data describing the transaction, digital signatures (certificates) identifying the parties to the transaction, and a tamper-proof seal (e.g. checksum on an encrypted coding of the contents of the electronic transaction document) that safeguards the authenticity of the electronic transaction document. Other information may appear in an electronic transaction document as required in various applications or legal jurisdictions. For example, electronic transaction documents typically include the date of issue or signing. A single electronic transaction document, bearing the digital signatures of all of the parties may be used to establish the transaction. In the alternative, a plurality of transaction documents considered together may establish the transaction, with each

electronic transaction document establishing separate aspects of the transaction. Electronic transaction documents may be transmitted over communication networks such as the Web.

As used herein, the entity that issues an electronic transaction document is referred to as the "issuer", and the entity that receives the electronic transaction document is issued is referred to as the "recipient." Generally, issuers and recipients are signatories who are parties to the transaction and are required to place their digital signatures on the electronic transaction documents. However, recipients may also include third party signatories, such as notaries or auditors, who are participants but not parties to the transaction.

Directing attention to Fig. 1, the Transaction Document System 10 enables electronic business transactions to be conducted across the World Wide Web 20 or other communication systems that support remotely located computer systems. The communication subsystem can include a web interface system, an e-mail system, (with or without its own cryptographic features), an EDI system, a private direct communication link, or any other communication subsystem, either separate from or built in to the Transaction Document System 10. The Transaction Document System 10 comprises a Transaction Document Server 30 implemented on an issuer's computer system, and a Transaction Document Client 70 implemented on a recipient's computer system. In general, the business logic of a transaction is implemented in the workflow system 90 and the Transaction Document Server 30 executes protocols for obtaining signatures. Depending on the application of the Transaction Document System 10, the API 40 may be customized to accommodate various workflow systems.

The Transaction Document Server 30 is implemented on the issuer's computer system and is used by the issuer to produce and publish an electronic transaction document bearing the issuer's digital signature. The Transaction Document Server 30 includes a set of computer instructions that, when executed by a computer system, executes the method of the present invention. The Transaction

Document Server 30 may be implemented as a service plug-in to a regular web server or commerce server using, for example, the servlet API, ISAPI or NSAPI. Protocols are executed for gathering signatures when the Transaction Document Server 30 receives a request from a commerce server or other workflow system 90 to generate an electronic transaction document for a Web-based transaction, or from a file server to generate an electronic transaction document to be transmitted with a file.

The Transaction Document Client 70 is implemented on the recipient's computer system and is used by recipients to receive and sign their copies of an electronic transaction document. The Transaction Document Client 70 includes a set of computer instructions that, when executed by a computer system, executes the method of the present invention. The Transaction Document Client 70 may be implemented as an extension to a file transfer client (such as the FileDrive client available from Differential, Inc., Cupertino, CA), or for web-based transactions, as a browser plug-in or Java applet. In the latter two cases, the Transaction Document Client 70 installs itself on the recipient's system such that it is invoked seamlessly when an electronic transaction document is received.

"Computer instructions" for performing various tasks as described herein can be stored on a non-volatile computer storage medium (e.g. hard drive, floppy disk, optical disk, or the like), or in a volatile computer storage medium, such as a computer's main memory or cache memory, or any combination or storage media, either in one location or spread over a number of locations.

The Electronic Transaction Document Server 30 and Client 70 include an Application Specific Interface (API) 40. The API 40 allows the Transaction Document Server 30 and/or Client 70 to communicate with outside application programs such as workflow systems 90. The API 40 provides connectivity to other software systems that utilize the Transaction Document System 10. The API 40 may contain three or more levels. These include a high level API, a low level API, and a workflow API. The high level API has a minimal set of calls, may include UI

components, and performs most of its functions through calls to the low level API. The low level API may be platform independent, and incorporates an extensive set of functions. As the low level is mostly used by the high level API, the low level API does not require a UI. The workflow API provides connectivity to the workflow 90, which may be an external commerce server or corporate workflow system. Additionally, a crypto API may be included, which hides differences between various API's which may be used by different systems such as BSAFE or MSCryptoAPI. The crypto API provides the low level API with platform independence.

The Transaction Document Server 30 and Client 70 may also provide a web-browser user interface (UI) 42 for recipients that allows them to sign and validate electronic transaction documents as well as track transmission and provide auditing functions. The UI 42 is described in detail below.

A validator module 44 may be incorporated into Transaction Document Server 30 and Client 70. The validator module 44 checks the validity of an electronic transaction document. The validator module 44 is called whenever an electronic transaction document is received, or it may be called as needed for auditing purposes. The validator module 44 validates each signature (certificate) on the electronic transaction document by verifying the certificate with the appropriate certificate authority (CA), e.g. Verisign. It also verifies that the contents of the electronic transaction document have not been altered, by validating the tamper-proof seal (i.e. the digital signature, the checksum on the encrypted contents of an electronic transaction document). The method of validation depends on the signing standard adopted for the particular embodiment. For example, OTP keeps separate checksums for different parts of the document, in this case, the validator module 44 would validate each section separately. Conversely, PKCS#7 does not keep a separate checksum in the clear, the validator module 44 has to reconstruct it from the message itself.

The Transaction Document Server 30 may also include a server administration module 46 provides screens that allow the administrative users to

perform the most important tasks of setting up, configuring and maintaining the Transaction Document Server 30. The administration module 46 provides a user interface that may be web-based, allowing for remote administration. Administrative functions include:

- Setting up the server port and connections parameters.
- Setting up the email configuration for sending messages and electronic transaction documents etc. to clients.
- Setting up initial parameters for encryption and the certificate to be used for signing electronic transaction documents and messages.
- Setting up the logging and auditing parameters for keeping track of all transactions and error messages.
- Database maintenance procedures for validity checking to see if any electronic transaction documents are corrupted or transactions were tampered with. Validation reports can be produced.
- Selection of document formats from a set of available templates. Templates can be created/edited with a separate template editor using XML tags.
- Create and modify user accounts for access to these administration pages and allocate appropriate levels of authorization.

The Data Definition 50 is utilized by both the Transaction Document Server 30 and Client 70. The Data Definition 50 contains libraries that describe the various representations of electronic transaction documents, and transformations from one representation to another. The Data Definition 50 specifies required data, optional data, and protocols for subclassing and adding data to electronic transaction documents. The transformation methods define the mapping between representations as required for compliance with different standards supported by the system. Representations include Internal, Database and Published.

The Data Definition 50 also includes a worldwide unique ID for each individual electronic transaction document, consisting of a combination of the

Issuer's Certificate Authority's ID, the Issuer's Certificate ID, and a tracking number generated by the Issuer. The Data Definition 50 may also include indexing "hooks" for associating electronic transaction documents with a Transaction ID, and for associating them with one another in sequential relationship (i.e. a chain of transaction documents) and replacement.

The Internal Representation 52 provides the classes for the various types of electronic transaction documents implemented on a Transaction Document Server 30 or Transaction Document Client 70. A generic transaction document class may be implemented on the Server 30 and Client 70, as well as other classes with specialized data and workflow behavior. Examples of the classes defined in the Internal Representation 52 are provided below.

The following examples of class definitions included in the Internal Representation 52 are provided for illustrative purposes only. It is to be understood that the following classes are not to be considered the entire set of class definitions contained in the Internal Representation 52. It is also to be understood that changes to the content and format of the class definitions contained in the Internal Representation 52 may be made without departing from the spirit of the invention.

```
<!-- Document Type Definition for Electronic Transaction Document
-->
<!-- class Digital Receipt -->
<?xml version = "1.0"?>
<!DOCTYPE digital_receipt [

<!-- List of the ELEMENTS (contents) of a Digital Receipt -->

<!-- The root element of a receipt document -->
<!-- NOTE that the digital signature(s) are appended to the receipt
-->
<!-- ^^ they cannot be described in the XML definition because they
are generated -->
<!-- ^^ from a document digest that encompasses the XML document.
-->

<!ELEMENT receipt
            (issuer,
             recipients,
```

```
                date_issued,
                date_signed?
                transaction,
                related_receipts,
                other_info
                )>

    <!ELEMENT issuer (signatory)>

    <!ELEMENT recipients (signatory)+>

    <!ELEMENT date_issued (date)>

    <!ELEMENT date_signed (date)>

    <!ELEMENT transaction
                (description,
                date
                )>

    <!ELEMENT related_receipts
                (receipt_ID,description?)*>

    <!-- ATTRIBUTES of the elements -->

    <!-- receipt -->
    <!ATTLIST receipt software_version CDATA #IMPLIED>
    <!ATTLIST receipt id ID #REQUIRED>
    <!ATTLIST receipt type CDATA #REQUIRED>
    <!ATTLIST status (UNISSUED, ISSUED, IN_PROCESS, FULLY_SIGNED,
    REJECTED) #REQUIRED>

    <!-- transaction -->
    <!ATTLIST transaction id ID #REQUIRED>
    <!ATTLIST transaction type CDATA #IMPLIED>
    <!ATTLIST transaction status CDATA #IMPLIED>

    <!-- signatory -->
    <!ATTLIST signatory id ID #REQUIRED>
    <!ATTLIST signatory name CDATA #REQUIRED>
    <!ATTLIST signatory description CDATA #IMPLIED>
    <!ATTLIST signatory role_in_transaction CDATA #IMPLIED>
    <!ATTLIST signatory logo CDATA #IMPLIED>

    <!-- date -->
    <!ATTLIST date year CDATA #REQUIRED>
    <!ATTLIST date month CDATA #REQUIRED>
    <!ATTLIST date day CDATA #REQUIRED>
    <!ATTLIST date hours CDATA #IMPLIED>
    <!ATTLIST date minutes CDATA #IMPLIED>
    <!ATTLIST date seconds CDATA #IMPLIED>

    <!-- receipt_ID in list of related_receipts -->
    <!ATTLIST receipt_ID id ID #REQUIRED>

    ]>  <!-- end of DOCTYPE receipt -->
```

```
<!-- Example of a Electronic Transaction Document Body -->

<?xml version = "1.0"?>
<!-- Receipt document type definition is external, in the file named
below -->

<!DOCTYPE SYSTEM "www.vereceipt.com/dtds/receipts/receipt.dtd">
<receipt
    software_version = "Vereceipt 0.01"
    id = "CA0199/853/4 CN1040/72/8901/009 TX04/0119/5307 RN00001"
    type = "Delivery"
    status = "IN_PROCESS"
    >
    <issuer>
        <signatory
            id = "CA0199/853/4 CN1040/72/8901/009"
            name = "Render Farms Inc."
            role_in_transaction = "Sender"
            >
    </issuer>

    <recipients>
        <signatory
            id = "CA0199/853/4 CN2478/85/4769/055"
            name = "Pacific Data Images"
            role_in_transaction = "Recipient"
            >
    </recipients>

    <date_issued>
        <date
            year = "1998"
            month = "09"
            day = "14"
            hours = "05"
            minutes = "47"
            />
    </date_issued>

    <transaction
        id = "TX04/0119/5307"
        type = "File Delivery"
        status = "Done:Receipt Pending"
        <description> "Delivery of file trainseq.ani"/>
        <date
            year = "1998"
            month = "09"
            day = "14"
            hours = "05"
            minutes = "44"
            />

    </transaction>
```

```
<related_receipts>
        <receipt_ID id = "CA0199/853/4 CN1040/72/8901/009
TX04/0119/5281 RN00001"/>
        <description "Request for service"/>
        <receipt_ID id = "CA0199/853/4 CN1040/72/8901/009
TX04/0119/5282 RN00001"/>
        <description "Receipt of materials"/>
        <receipt_ID id = "CA0199/853/4 CN1040/72/8901/009
TX04/0119/5290 RN00001"/>
        <description "Payment"/>
</related_receipts>
```

The Database Representation 54 provides relational database specifications for fields corresponding to members of the aforementioned class(es), and tables establishing relations among electronic transaction documents (e.g. chains) and between electronic transaction document contents and external data. These specifications may follow standard SQL.

The Published Representation 56 describes an electronic transaction document as it is transmitted between issuer and recipient. It uses an eXtended Markup Language (XML) notation, following the electronic transaction document data format given in the Open Trading Protocol (OTP) standard.

The published representation 56 describes both the embedded data to be read by the Transaction Document Server 30, Transaction Document Client 70, and workflow system 90, and the appearance of an electronic transaction document (as in a web browser). The organization of the embedded data is referred to herein as the formal electronic transaction document. The electronic transaction document as it appears is referred to herein as the visible electronic transaction document. The formal electronic transaction document consists of a document encoded according to a known BER (Binary Encoding Rules) standard, and signed according to the PKCS#7 standard for signing documents. It contains the data elements listed below.

Each signature in an electronic transaction document may contain several information fields, in addition to the usual signature algorithm identifiers, signature certificate references and the encrypted digest itself. These fields may include: date of signing (UTC), meaning of signature (a coded field with values related to

received, acknowledged, fulfilled, etc.), and an optional comment. These extra fields may be added to the signed part of the electronic transaction document.

For cases in which the issuer knows that the recipient will be using compatible software to process the electronic transaction document, the formal electronic transaction document may be all that is needed. However, if the recipient's software is unknown or known to be incompatible, an alternative form of the electronic transaction document, or multiple alternative forms, may be delivered along with the formal electronic transaction document.

Each visible form also carries a short message explaining: the importance of the signed, non-repudiable electronic transaction document, how to save the electronic transaction document, including the formal electronic transaction document to a disk file in commonly used software, how to obtain client software for electronic transaction document validation, etc.

Electronic transaction documents can be embodied in different forms transmitted via a number of different transport mechanisms, such as HTTP (for the Web), via FTP (for FileDrive) or by E-mail (for offline interchange).

In the case of HTTP and FTP, the forms sent are determined by content negotiation. MIME may be used to combine the multiple forms. Additionally, the formal electronic transaction document may be encapsulated in an S/MIME package by base64 encoding and attachment of appropriate headers.

The formal electronic transaction document may be generated by hierarchical construction of the electronic transaction document data below as an XML document. This is then canonicalized according to the process defined in the OTP preliminary specification (elimination of white space, etc). The canonical XML object is digested, and the digest is signed by the issuer (e.g. according to XML canonicalisation algorithm contained in OTP spec (OTP Func. Spec. v0.9, scn3.13.6.2)). Finally, the XML object, and the version identifier, digest algorithm identifiers, certificates, certificate revocation lists, and signer information (including the signature) are packaged as a BER object according to the PKCS#7 rules. The

signing and packaging process may be recursively repeated to attach the recipient's signature if multiple signatories are involved.

The data contained in the electronic transaction document may also be contained in an XML document constructed hierarchically from the following data items according to an XML document type definition. The document type definition and the exact tags to be used conform closely to either the XML/EDI guidelines or to the OTP proposed specification. Electronic transaction document data may include:

software version information (used to maintain backwards compatibility); type of electronic transaction document (includes information used to decide on future processing, for example whether this electronic transaction document requires further signing); references to related electronic transaction documents; a unique electronic transaction document ID; and content of the electronic transaction document.

The content of electronic transaction document may include a description of the issuer and recipients, date of issue, date the first signature was affixed to the document, description of the transaction, decorations to be included in the visible form of the document, and the layout of the visible form.

The issuer's certificate may be sent as part of the electronic transaction document. A unique reference to the issuer's certificate, consisting of the certificate issuing authorities distinguished name composed with the issuer's distinguished name as given in the certificate, is sent with the electronic transaction document as part of the signature information defined by the PKCS#7 specification.

As with the issuer's certificate, the recipient's certificate may be sent as part of the returning electronic transaction document. A unique reference to the recipient's certificate, consisting of the certificate issuing authorities distinguished name composed with the recipient's distinguished name as given in the certificate, is sent with the returning electronic transaction document as part of the signature information defined by the PKCS#7 specification.

The Transaction Document Server 30 and Transaction Document Client 70 each incorporate a database 60. The database 60 includes a signatories table 62, a transaction document table 64, and a transaction documents relations table 66. Received transaction documents and messages are stored in the transaction documents table 64. The transaction documents relations table stores chains of indexing hooks that reference associated electronic transaction documents.

Fig. 2 is an illustration depicting the structure of an electronic transaction document as used in accordance with the present invention. The core aspects of the electronic transaction document 200 include the contents 202 that are issued by the Transaction Document Server 30, the encrypted digest 204, and digital signature 206. The contents 202 may name the parties and contain the terms of the transaction, or reference the terms contained in a separate document. The contents 202 are secured by digest 204 and the issuer's digital signature 206. The contents 202, document digest 204 and signature 206 are sent to the Transaction Document Client 70, who verifies one or more of them and adds an additional document digest 214 and signature 216. It is to be understood that the electronic transaction document 200 is one of a variety of different types of electronic transaction documents that may be implemented by the Transaction Document System 10, and various other signature arrangements are discussed in detail below.

Fig. 3 is a flow chart illustrating the logical sequence of steps executed to create and transmit an electronic transaction document and obtain a digital signature from a single recipient as shown in Fig. 2. Directing attention to step 300, the Transaction Document Server 30 prepares transaction document content, comprising a Transaction Document ID number, Description of the Issuer, Description of the Transaction, Description of the recipient, and references to other transaction documents. The content optionally refers to one or more previous transactions (via their unique identifiers) to which this transaction is related. Transaction content usually describes or refers to contractual terms of the transaction (e.g. describing items purchased, price, etc.); describes all parties to the transaction, including their

name and (possibly a unique identifier, and role in the transaction; and requests the recipient to sign and return a copy of the electronic transaction document. Transaction document content is supplied to the Transaction Document Server 30 from the workflow system 90 via API 40.

Continuing to step 302, the Transaction Document Server 30 then inserts the issuer's digital signature into the electronic transaction document and encrypts the electronic transaction document, using the Issuer's certificate (such as available from Verisign) and generating a digest on the encrypted form of the electronic transaction document content. The digital signature verifies the identity of the participant and indicates agreement to the terms described or implied in the electronic transaction document. Signing is the means by which the identity of the issuer is rendered non-repudiable. The method for signing XML documents proposed for OTP is described in the Open Trading Protocol Specification, Ver. 0.9, Jan. 12, 1998, incorporated herein by reference. The issuer then generates a tamper proof seal by creating, for example, an encrypted checksum on an encrypted encoding of the electronic transaction document's contents. This tamper proof seal is the means by which the content of the electronic transaction document is rendered non-repudiable. The issuer then encrypts the electronic transaction document for transmission. Encryption can take place at the OPR level or at the level of the communication subsystem, or both, and the communication subsystem may or may not add its own further cryptographic functions. The functions of the communication subsystem when not shown explicitly or described in this or other flowcharts herein or in their accompanying descriptions, should be understood to be present nevertheless.

At step 304 the Transaction Document Server 30 transmits the electronic transaction document to the Transaction Document Client 70. This transmission may be implemented using the Secure Socket Layer (SSL). The electronic transaction document can also be sent using any network protocol such as HTTP, HTTPS, FTP, SMIME email, etc. The Transaction Document Server 30 may also

notify the workflow 90 that an electronic transaction document has been issued and a signature is pending.

At step 306 the Transaction Document Client 70 receives and decrypts the electronic transaction document. Control continues to step 308, where the Transaction Document Client 70 validates the issuer's digital signature. If the digital signature is invalid, indicating either a false identity or the contents of the electronic transaction document have been compromised, the Transaction Document Client 70 rejects the electronic transaction document, notifying both the recipient (step 312) and the Transaction Document Server 30 (step 314), which in turn notifies the issuer.

If the issuer's signature is valid, the Transaction Document Client 70 presents the document to the recipient for review (step 310). The recipient may be either a person, viewing the document in a browser or email message, or an automated system, parsing the XML-tagged data fields of the document.

The recipient may decide either to accept or reject the electronic transaction document or delay this decision. It is to be understood that acceptance of the electronic transaction document indicates acceptance of the *content* or terms contained in the electronic transaction document; it is not merely an acknowledgment that the electronic transaction document was received. Depending on the application, the recipient may also be able to add some data to the electronic transaction document, such as a date-of-signature timestamp.

If the recipient decides to reject the electronic transaction document, control proceeds to step 316, where the rejection protocol is executed. The rejection protocol is explained in more detail below with reference to Fig. 4.

If the recipient decides to accept the electronic transaction document, he or she first carries out any actions required by the electronic transaction document. In particular, the electronic transaction document may include required data entry fields or requests to obtain and submit other documents (such as notarized transaction documents or affidavits) and cite their reference numbers on the electronic transaction document. In the either case, the actions may require some

time to complete and the recipient may choose to delay signing and returning the electronic transaction document. At step 318 the Transaction Document Client 70 stores the transaction document in its database 60, so that the recipient may retrieve it when ready to sign. The Transaction Document Client 70 then notifies the Transaction Document Server 30 (step 320) of the delay. At step 322, the Transaction Document Server 30 makes an entry in the transaction documents table 64 reflecting that the recipient is deferring signing, and notifies the issuer at step 324.

Once the electronic transaction document has been reviewed and any required actions completed, the Transaction Document Client 70 signs the electronic transaction document with the recipient's digital signature (step 326), thereby authenticating it and sealing any added content against tampering. This signed electronic transaction document is referred to herein as an acceptance message, and refers to the unique transaction identifier on the original electronic transaction document and indicates acceptance of the terms. The acceptance message may or may not include all the terms or other information contained in the original electronic transaction document, depending on the particular application. At step 328, the Transaction Document Client 70 stores a copy of the acceptance message in its transaction document table 64. The Transaction Document Client 70 then encrypts and transmits the acceptance message back to the Transaction Document Server 30 (step 330). This transmission may also be implemented using SSL, and may transmit copies of it to third parties, such as auditors. Depending on the embodiment, this routing to third parties could be handled by the Transaction Document Server 30 or left to the workflow system. The Transaction Document Server 30 may perform the optional steps of creating and sending to the Transaction Document Client 70 an acknowledgment message.

Directing attention to Fig. 4, when the recipient rejects the electronic transaction document (step 400), the Transaction Document Client 70 prepares a rejection message (step 402). The rejection message is an electronic transaction document that refers to the unique transaction identifier on the original electronic

transaction document and indicates rejection of the terms. At step 404, the recipient signs the rejection note with his or her digital signature. The rejection message is then encrypted (step 406) and transmitted to the Transaction Document Server 30 (step 408). The Transaction Document Server 30 receives the encrypted rejection message (step 410), decrypts and validates the message (step 412). If the recipient's signature is invalid, the Transaction Document Server 30 reports to the workflow system 90 (step 414) and the Transaction Document Client 70 (step 416) that the signature is invalid. If the recipient's signature is valid, the Transaction Document Server 30 reports to the workflow system 90 that the original transaction document sent to the Transaction Document Client 70 was rejected by the recipient (step 418). The Transaction Document Server 30 may perform the optional steps of creating and sending to the Transaction Document Client 70 an acknowledgment message.

An electronic transaction document may contain multiple digital signatures. For example, approval cycles or notarization of the transaction may require third party signatures. Signatures may be applied in parallel or cascaded. A cascaded signature testifies that the signatory has inspected the other signatures, and once a cascaded signature has been applied to an electronic transaction document, no additional parallel signatures can be permitted above the cascaded signature. However, other signatures may be applied in parallel to the cascaded signature and a further level (or levels) of cascaded signatures may be added.

Different protocols for collecting multiple signatures for an electronic transaction document may be executed by the Transaction Document System 10. The Parallel Protocol (Fig. 5a) sends copies of the electronic transaction document to all signatories concurrently, and then collates the responses onto a single final-issue electronic transaction document. The Serial Protocol (Fig. 5b) passes the electronic transaction document to each signatory in turn, so that each digital signature encloses the previous one. In both the Parallel and Serial protocols, the procedure for gathering each signature is similar to steps 304 - 334 described in Fig. 3. The Serial Protocol differs from the Parallel Protocol in that the Serial

Protocol may abort the signature gathering process if any one signatory rejects or submits an invalid document. It notifies the workflow system, which decides whether to continue gathering other signatures.

Directing attention to Fig. 5a, the Transaction Document Server 30 prepares transaction document content at step 500 and inserts the issuer's digital signature into the electronic transaction document and encrypts the electronic transaction document at step 502. Steps 500 and 502 are performed in a similar manner as described in steps 300 and 302 of Fig. 3. Continuing to step 504, for each of the recipients involved in the multiple signature parallel protocol, similar steps enumerated in steps 304 - 334 of Fig. 3 are performed. If one or more of the received response messages contain an invalid signature, control proceeds to step 506, where receipt of the invalid signature is reported to the workflow 90 and the client (508). The optional step 510 may be included where the Transaction Document Server 30 stores the partially signed document in the transaction documents table 64. However, if all of the recipients have responded with properly signed response messages, control proceeds to step 512, where the Transaction Document Server 30 embeds all of the received documents in the original electronic transaction document. The fully signed document is stored in the transaction document table 64 at step 514 and the workflow 90 is notified at step 516 that all recipients have signed the document. The fully signed document is encrypted at step 518, and copies are sent to each of the recipients at step 520. Completing the protocol at step 522, each of the individual Transaction Document Clients 70 belonging to the recipients validates the received fully signed document and stores it in transaction documents table 64.

A cascaded signature testifies that the signatory has inspected the other signatures, and once a cascaded signature has been applied to an electronic transaction document, no other parallel signatures can be permitted. However, other signatures may be applied in parallel to the cascaded signature (with the same meaning) and a further level (or levels) of cascaded signatures may be added.

Directing attention to Fig. 5b, the serial protocol is executed to obtain cascaded signatures. The Transaction Document Server 30 prepares transaction document content (step 550), inserts the issuer's digital signature into the electronic transaction document and encrypts the electronic transaction document (step 502). Steps 500 and 502 are performed in a similar manner as described in steps 300 and 302 of Fig. 3. Continuing to step 554, for the first signatory in the serial protocol, a signature collection procedure is executed, similar to the steps enumerated in steps 304 - 334 of Fig. 3. If the received response message contains an invalid signature, control proceeds to step 556, where receipt of the invalid signature is reported to the workflow 90 and the client 70 (step 558). The optional step 560 may be included where the Transaction Document Server 30 stores the partially signed document in the transaction document table 64. If the recipient responded with a properly signed response message, control proceeds to step 562, where the Transaction Document Server 30 embeds the received signature into the original electronic transaction document. To send the partially signed document to the next signatory in the chain, control returns to step 552, where the partially signed document is signed and encrypted. This sequence is repeated for the remaining signatories. When the chain is complete and all signatures have been received, the fully signed document is stored in the transaction document table 64 at step 564 and the workflow 90 is notified at step 566 that all recipients have signed the document. The fully signed document is encrypted at step 568, and copies are sent to each of the recipients at step 570. Completing the protocol at step 572, each of the individual Transaction Document Clients 70 belonging to the recipients validates the received fully signed document and stores it in its own database.

NON-PARTY PARTICIPANTS

Some transaction documents, such as purchase orders for amounts above a set amount, may require the signatures of non-party participants, such as notaries, supervisors, or similar entities to complete a transaction. The present invention

implements these types of transactions in an online setting by allowing non-party participants to use the Transaction Document System 10 to affix his or her digital signature to the electronic transaction document. Figs. 6a and 6b illustrate the logical sequence of steps executed by the present invention to accommodate the signatures non-party participants in electronic transaction documents. For illustrative purposes, these examples incorporate the digital signature of a notary, but other non-party participants may be used as well.

Fig. 6a is a flowchart illustrating the logical sequence of steps that execute a notarized transaction according to the present invention. In this scenario, a notary participates in the transaction between a merchant (issuer) and customer (recipient). The merchant and customer are conducting transactions surrounding the sale of goods or services. The merchant uses a Transaction Document Server 30, and the customer and notary use separate Transaction Document Clients 70. Directing attention to step 600, the Transaction Document Server 30 creates an electronic transaction document, affixes the merchant's digital signature, and encrypts the document in a similar manner as described in steps 300-302 of Fig. 3. At step 602, the issuer transmits the electronic transaction document to the notary. This transmission may be implemented using the Secure Socket Layer (SSL). The electronic transaction document can also be sent using any network protocol such as HTTP, HTTPS, FTP, SMIME email, etc. The Transaction Document Server 30 may also notify the workflow 90 that an electronic transaction document has been issued and a signature is pending. At step 604, the notary receives and verifies the electronic transaction document. The notary's Transaction Document Client 70 then encrypts a checksum of the electronic transaction document and notarizes the electronic transaction document by affixing its digital signature to the electronic transaction. The notary may also store a copy of the electronic transaction document in a database for future reference. At step 606, the notary transmits the notarized electronic transaction document back to the merchant. The merchant receives the notarized electronic transaction document at step 608. The merchant may verify the

signature of the notary and store it in a database for future reference and proof that the electronic transaction document was notarized. At step 610, the merchant transmits the electronic transaction document to the customer. The merchant may send either the original electronic transaction document or the notarized electronic transaction document, depending on the business requirements. At step 612, the customer receives the electronic transaction document and verifies the digital signature of the merchant. The customer may also verify the notary's digital signature, if the notary's signature was appended to the electronic transaction document. The customer may then process the electronic transaction document. Processing the document may include storing it in a database for future reference, presenting the electronic transaction document to a user who could interactively approve or deny the electronic transaction document, or entering the document into a purchasing system, accounting system or document management system. At step 614, the customer generates an electronic transaction document that responds to the received electronic transaction document. This response can be either an approval, denial or pending notification. The response can optionally refer to the original electronic transaction document by its ID number, or the checksum and signature of the merchant, or by the notary. Alternatively, the response can actually contain the original electronic transaction document itself as part of the response electronic transaction document. The response electronic transaction document is checksummed and signed with the customer's private key. The response is then transmitted to the merchant. At step 616, the merchant receives the electronic transaction document response from the customer. The merchant then processes the electronic transaction document response. Processing may include verifying the customer's digital signature, storing the electronic transaction document response for future reference, entering the response into an order processing system, and the like. At step 618, the merchant transmits a copy of the electronic transaction document response to the notary. The merchant may affix his digital signature the electronic transaction document before sending. At step 620, the notary receives the

electronic transaction document response from the merchant. The notary may then verify the signatures of the merchant and customer, and reconcile the electronic transaction document response with the original electronic transaction document. The notary may also store the response in a database for future reference. At step 622, the notary transmits a response message back to the merchant indicating that the customer's response was notarized and recorded. The notary's response message may also be an electronic transaction document. The notary's response may contain simply a reference to the original electronic transaction document and the electronic transaction document response from the customer, or it may contain the actual original electronic transaction document and the electronic transaction document response. At step 624, the merchant receives the notary's response message. The merchant may then verify the notary's digital signature and initiate or complete a transaction, such as shipping goods, performing services and the like.

The explanation above describes a process in which an electronic transaction document must be notarized before sending, the delivery and approval/denial/pending of the electronic transaction document is notarized, and the entire process must be completed before the transaction is finalized. Alternatively, the merchant could start the process when the electronic transaction document response is received from the customer in step 616, and the final notarization could be performed for record keeping purposes only. The merchant could also process the transaction after step 616, and attach the results of that transaction to the message that is sent in step 618 to the notary to provide evidence that the transaction was originated, received and processed. If desired, the process illustrated in Fig. 6a may be executed once for the initiation of the order and a second time for the completion of the transaction.

Fig. 6b describes an alternative notarization protocol which is similar to the protocol described in Fig. 6a, but includes interaction with two separate notaries. This allows both parties (merchant and customer) involved in the transaction to have the entire process audited by their own trusted third party. The notaries may

collectively reconcile the transactions between the merchant and customer. In this protocol, it is assumed that the merchant has selected notary A and the customer has selected notary B. Again, the merchant uses the Transaction Document Server 30, and the customer, notary A and notary B each use their own Transaction Document Client 70. Directing attention to step 650, the merchant's Transaction Document Server 30 creates the electronic transaction document, affixes the merchant's digital signature, and encrypts the document in a similar manner as described in steps 300-302 of Fig. 3. At step 652, the merchant transmits the electronic transaction document to notary A. This transmission may be implemented using the Secure Socket Layer (SSL). The electronic transaction document can also be sent using any network protocol such as HTTP, HTTPS, FTP, SMIME email, etc. The Transaction Document Server 30 may also notify the workflow 90 that an electronic transaction document has been issued and a signature is pending. At step 654, notary A receives and verifies the electronic transaction document. Notary A's Transaction Document Client 70 then encrypts a checksum of the electronic transaction document and notarizes the electronic transaction document by affixing its digital signature to the electronic transaction. Notary A may also store a copy of the electronic transaction document in a database for future reference. At step 656, notary A transmits the notarized electronic transaction document back to the merchant. The merchant receives the notarized electronic transaction document at step 658. The merchant may verify the signature of notary A and store the notarized document in a database for future reference and proof that the electronic transaction document was notarized. At step 660, the merchant transmits the electronic transaction document to the customer. The merchant may transmit either the original electronic transaction document or the notarized electronic transaction document, depending on the business requirements. At step 662, the customer receives the electronic transaction document and verifies the digital signature of the merchant. The customer may also verify notary A's digital signature, if notary A's signature was appended to the electronic transaction document. The customer may then process the electronic

transaction document. Processing the document may include storing it in a database for future reference, presenting the electronic transaction document to a user who could interactively approve or deny the electronic transaction document, or entering the document into a purchasing system, accounting system or document management system. At step 664, the customer generates an electronic transaction document that responds to the received electronic transaction document. This response can be either an approval, denial or pending notification. The response can optionally refer to the original electronic transaction document by its ID number, or the checksum and signature of the merchant, or the notary. Alternatively, the response can actually contain the original electronic transaction document itself as part of the response electronic transaction document. The response electronic transaction document is checksummed and signed with the customer's private key. The response is then transmitted to notary B. At step 666, Notary B receives and verifies the response, and notarizes the response by creating a digest of the response and signing the response and its digest with its private key. Notary B may also store a copy of the response in a database for future reference. At step 668, notary B transmits the notarized response back to the customer. At step 670, the customer receives the notarized response and may verify the signature of notary B. The customer may store the notarized response in a database for future reference and proof that the document was notarized. At step 672, the customer transmits the response to the merchant. The customer may send the original electronic transaction document response or the notarized response. At step 674, the merchant receives the response from the customer. The merchant may then verify the digital signature of the customer and process the response. Processing may include storing the response for future reference, processing by an order processing system, etc. At step 676, the merchant transmits a copy of the response to notary A. The merchant may sign the response before sending. At step 678, notary A receives the response from the merchant. Notary A may verify the signatures contained in the response, reconcile the response with the original electronic transaction document, and attach

its digital signature to the response. Notary A may also store this document in a database for future reference. At step 680, notary A transmits a message back to the merchant indicating that the customer's response was notarized and recorded. This message may also be a electronic transaction document, and may contain simply a reference to the original electronic transaction document and the response from the customer, or it could contain the actual original electronic transaction document and the response. At step 682, the merchant receives the message from notary A, and may verify notary A's digital signature. The merchant then processes the message. This could mean actually initiating or completing a transaction. Similar alternatives are available as those set forth above with respect to the notarized transaction illustrated in Fig. 6a.

While Figs. 6a and 6b describe the interaction of notaries in the operation of the Transaction Document System 10, other third party signatories such as auditors may be substituted for notaries in the above examples.

VERIFICATION

When an electronic transaction document is received, either by the Transaction Document Client 70 when the document is issued by the Transaction Document Server 30, or when the Transaction Document Server 30 receives a response and is required to sign and retransmit the document, the UI 42 may be summoned by the user to display the document. Directing attention to Fig. 7a, the UI 42 displays screen 700. The electronic transaction document is displayed in window 702. The user may view the contents of the document, or print the document. The user may press the accept button 704, the delay signing button 706, or the reject button 708. Screen 700 thus allows a user to manually control the acceptance or rejection of the electronic transaction document. Again, it is to be understood that acceptance or rejection refers to acceptance or rejection of the contents or terms of the document rather than acceptance or rejection of the delivery of the document. In cases of high volume document traffic, the UI 42 may be

configured to perform the accept/reject/delay process automatically. The show related button 710 allows a user to view a list of stored electronic transaction documents that are related to the currently displayed document (Fig. 7c).

In addition to accepting and rejecting received electronic transaction documents, the UI 42 provides auditing functions for tracking, verifying, and generating reports on electronic transaction documents stored in the database 60. By pressing the select document button 712, screen 720 (Fig. 7b) appears and displays information related to the transmission of electronic transaction documents and related responses. The displayed information may be used to ensure delivery and to verify acceptance or rejection. The user may choose to track all documents, or documents of a selected status, such as accepted documents, failed transmissions, rejected documents, or indeterminate transmissions. Additionally, the user may specify a date from which tracking is performed. Once the above selections have been made, a list of documents matching the user's query are displayed below, organized by fields. The fields may include document description, which is usually an identifier that has been attached to a particular document, customer name, date and time the document was issued, status, and a field indicating whether related documents exist.

If a user wishes to view the list of related documents, pressing the Show Related Documents button 722 will summon the Related Documents Screen 730 (Fig. 7c). By pressing the link documents button 724, the user is guided through a process that allows the user to view lists of stored documents, select documents, and establish links between the selected documents and the current electronic transaction documents. The list of currently linked documents may then be displayed on the Related Transaction Documents Screen 730. Alternatively, the workflow 90 may automatically establish the relationships between electronic transaction documents according to their role in a transaction. Links between electronic transaction documents may also be removed through a similar process by pressing the remove

links button 726. Manipulating links between electronic transaction documents may be performed on both the Transaction Document Server 30 or Server 70.

The UI 42 also allows a user to audit any document or group of documents stored the database 60. By pressing the audit transaction documents button 728, the validator module 44 is invoked to verify that a selected document or group of documents has not been altered since the putative date of issue and that signature certificates are valid. The results may be presented to the user in tabular form. Electronic transaction documents held by separate parties be reconciled in this manner to verify that they are identical.

Screen 730 displays and organizes a list of documents related to a document selected from screen 720 according to reference number, type, date of issue, and issuer name. Other information may also be displayed if desired. Since cross-references to electronic transaction documents may form an unbounded network, an electronic transaction document network containing only direct references to and from the current electronic transaction document are displayed. The user may then explore the chain(s) by selecting another electronic transaction document and expanding it in turn.

References commonly form sequences because transactions are sequenced, and recent references are usually the most relevant. The UI 42 also may display a subset of the electronic transaction document network, fanning out from the current electronic transaction document and including electronic transaction documents of relevant types. The search may be both breadth- and depth-bounded (for instance, stop at an electronic transaction document that connects to more than two others). Items at the end of the displayed portion of a branch may be marked (e.g. with ellipses, highlighting, shading, etc.) to indicate that the user can view more by selecting them. For example, the documents related to PO Confirmation 1457 may be selected according to the following rules:

1) Include electronic transaction documents directly connected to the current selection

2) Include electronic transaction documents involved in a Purchase Order workflow (that is, whose type is one of: PO, PO Confirmation, Sales Draft, APR, or Delivery)

3) Exclude all other electronic transaction documents

Fig. 7d is a flowchart showing the steps required to audit electronic documents stored in the electronic transaction documents table 64. At step 790, the user selects electronic transaction documents from the list displayed in screen 720. Selection may be performed by manipulating a mouse or other pointing device included in the computer system, or by pressing keys on a keyboard. At step 792, once the desired selections have been made from the list, the user selects the audit transactions button 728. By pressing the audit transactions button 728 when electronic transaction documents have been selected from the list, each selected document is passed to the the Validator module 44. The Validator module 44 inspects the digital signatures and encrypted digests covering the documents and notes whether any documents are unsigned, have been tampered with since the documents were signed, or suffer other verification problems. At step 794, the results of the audit are reported to the user. Reporting may achieved through a variety of methods, such as displaying or printing a report file, constructing and displaying a table containing fields such as document name and the result of the audit for the document, or other meaningful representations of the auditing results.

Fig. 8 is high-level block diagram view of an embodiment of a computer system having a computer program that causes the computer system to perform the method of the present invention. The Transaction Document Server 30 and the Transaction Document 70 are both implemented on computer systems such as the one shown in Fig. 8. The computer system 846 includes a processor 830 and memory 825. Processor 830 may contain a single microprocessor, or may contain a plurality of microprocessors for configuring the computer system as a multi-processor system. Memory 825, stores, in part, instructions and data for execution by processor 830. If the system of the present invention is wholly or

partially implemented in software, including a computer program, memory 825 stores the executable code when in operation. Memory 825 may include banks of dynamic random access memory (DRAM) as well as high speed cache memory.

The system 846 further includes a mass storage device 835, peripheral device(s) 840, input device(s) 855, portable storage medium drive(s) 860, a graphics subsystem 870 and a display 885. For simplicity, the components shown in Fig. 8 are depicted as being connected via a single bus 880. However, the components may be connected through one or more data transport means. For example, processor 830 and memory 825 may be connected via a local microprocessor bus, and the mass storage device 835, peripheral device(s) 840, portable storage medium drive(s) 860, and graphics subsystem 870 may be connected via one or more input/output (I/O) buses. Mass storage device 835, which is typically implemented with a magnetic disk drive or an optical disk drive, is a non-volatile storage device for storing data and instructions for use by processor 830. In another embodiment, mass storage device 835 stores the computer program implementing the method of automating a microelectronic manufacturing process for purposes of loading such computer program to memory 825. The method of the present invention also may be stored in processor 830.

Portable storage medium drive 860 operates in conjunction with a portable non-volatile storage medium, such as a floppy disk, or other computer-readable medium, to input and output data and code to and from the computer system 846. In one embodiment, the method of the present invention for automating a microelectronic manufacturing process is stored on such a portable medium, and is input to the computer system 846 via the portable storage medium drive 860. Peripheral device(s) 840 may include any type of computer support device, such as an input/output (I/O) interface, to add additional functionality to the computer system 846. For example, peripheral device(s) 840 may include a network interface card for interfacing computer system 846 to a network, a modem, and the like.

Input device(s) 855 provide a portion of a user interface. Input device(s) 855 may include an alpha-numeric keypad for inputting alpha-numeric and other key information, or a pointing device, such as a mouse, a trackball, stylus or cursor direction keys. In order to display textual and graphical information, the computer system 846 includes graphics subsystem 870 and display 885. Display 885 may include a cathode ray tube (CRT) display, liquid crystal display (LCD), other suitable display devices, or means for displaying, that enables a user to interact with the computer program to configure the application objects and implement the workflows. Graphics subsystem 870 receives textual and graphical information and processes the information for output to display 885. Display 885 can be used to display an interface to interact with the computer program to configure the application objects and implement the workflows and/or display other information that is part of a user interface. The display 885 provides a practical application of the method of automating a microelectronic manufacturing process since the method of the present invention may be directly and practically implemented through the use of the display 885. Additionally, the system 846 includes output devices 845. Examples of suitable output devices include speakers, printers, and the like.

The devices contained in the computer system 846 are those typically found in general purpose computer systems, and are intended to represent a broad category of such computer components that are well known in the art. The computer system of Fig. 8 illustrates one platform which can be used for practically implementing the method of the present invention. Numerous other platforms can also suffice, such as Macintosh-based platforms available from Apple Computer, Inc., platforms with different bus configurations, networked platforms, multi-processor platforms, other personal computers, workstations, mainframes, navigation systems, and the like.

Alternative embodiments of the use of the method of the present invention in conjunction with the computer system 846 further include using other display means for the monitor, such as CRT display, LCD display, projection displays, or the like. Likewise, any similar type of memory, other than memory 825, may be used.

Other interface apparatus, in addition to the component interfaces, may also be used including alpha-numeric keypads, other key information or any pointing devices such as a mouse, trackball, stylus, cursor or direction key.

It can be seen that the invention is not limited to use on any single platform, and may be configured for use with specialized business applications. While the invention has been described with respect to specific embodiments thereof, it is to be understood that numerous modifications are possible within its scope.

CLAIMS

1. A method for establishing a transaction, comprising the steps of:

engaging in a transaction involving at least first and second party participants and at least a first non-party participant;

providing to said first non-party participant an electronic transaction document, non-repudiable by said first party participant and describing said transaction;

in response to verification by said first non-party participant of at least one aspect of said electronic transaction document, adding an indication of said verification to said electronic transaction document and providing said electronic transaction document to said second party participant; and

in response to acceptance by said second party participant of said transaction as described in said electronic transaction document, providing to said first party participant an acceptance note, non-repudiable by said second party participant and evidencing acceptance of said transaction by said second party participant.

2. A method according to claim 1, further comprising the step of said second party participant indicating manually said acceptance of said transaction.

3. A method according to claim 1, wherein said step of providing said electronic transaction document comprises the step of affixing a digital signature of said first party participant to said electronic transaction document.

4. A method according to claim 1, wherein said step of verifying said electronic transaction document comprises the step of affixing a digital signature of said first non-party participant to said electronic transaction document.

5. A method according to claim 1, wherein said step of providing said electronic transaction document to said second party participant comprises the step of including with said electronic transaction document an encrypted digest covering at least part of said electronic transaction document.

6. A method according to claim 1, wherein said step of providing said acceptance note comprises the step of affixing a digital signature of said second party participant to said acceptance note.

7. A method according to claim 1, wherein said step of providing said acceptance note comprises the step of including with said acceptance note an encrypted digest covering at least part of said acceptance note.

8. A method according to claim 1, further comprising the step of, in response to receipt of said acceptance note, providing a response acknowledgment to said second party participant acknowledging receipt of said acceptance note.

9. A method according to claim 8, wherein said step of providing said response acknowledgment comprises the step of verifying adequacy to said first party participant of said acceptance note, and wherein said response acknowledgment further acknowledges adequacy of said acceptance note to said first party participant.

10. A method according claim 1, wherein said step of providing said acceptance note to said first party participant further comprises the steps of providing said acceptance note to a second non-party participant, and in response to verification of said acceptance note by said second non-party participant, adding an indication of said verification to said acceptance note before providing said acceptance note to said first party participant.

11. A method according to claim 10, wherein said step of adding an indication of verification to said acceptance note comprises the step of affixing a digital signature of said second non-party participant to said acceptance note.

12. A computer readable storage medium for use with computer apparatus, said medium carrying computer instructions which, when executed by said computer apparatus:

(a) provide an electronic transaction document from an issuer party participant to a first non- party participant, said document being non-repudiable by said issuer party participant and describing a transaction between said issuer party participant and at least one recipient party participant;

(b) in response to verification by said non-party participant of at least one aspect of said electronic transaction document, add an indication of said verification to said electronic transaction document and provide said electronic transaction document to said recipient party participant; and

(c) in response to acceptance by said recipient party participant of said transaction as described in said electronic transaction document, provide to said issuer party participant an acceptance note, non-repudiable by said recipient party participant and evidencing acceptance of said transaction by said recipient party participant.

13. A medium according to claim 12, wherein said electronic transaction document contains terms of said transaction.

14. A medium according to claim 12, wherein said electronic transaction document contains at least one reference to terms of said transaction.

15. A medium according to claim 12, wherein said electronic transaction document includes a digital signature of said issuer party participant.

16. A medium according to claim 12, wherein said electronic transaction document includes a digital signature of said non-party participant.

17. A medium according to claim 12, wherein said electronic transaction document includes an encrypted digest covering at least part of said electronic transaction document.

18. A medium according to claim 12, wherein said acceptance note includes a digital signature of said recipient party participant.

19. A medium according to claim 12, wherein said acceptance note includes a digital signature of at least one non-party participant.

20. A medium according to claim 12, wherein said acceptance note includes an encrypted digest covering at least part of said acceptance note.

21. A computer readable storage medium for use with computer apparatus, said medium carrying computer instructions which, when executed by said computer apparatus:

(a) provide an electronic transaction document to a first non-party participant, said document being non-repudiable by an issuer party participant and describing a transaction between said issuer party participant and at least one recipient party participant;

(b) in response to verification by said non-party participant of said electronic transaction document, receive said electronic transaction document and indication of said verification;

(c) provide said electronic transaction document and said indication of verification to said recipient party participant; and

(d) in response to acceptance by said recipient party participant of said transaction as described in said electronic transaction document, receive an acceptance note, non-repudiable by said recipient party participant and evidencing acceptance of said transaction by said recipient party participant.

22. A medium according to claim 21, wherein said electronic transaction document contains terms of said transaction.

23. A medium according to claim 21, wherein said electronic transaction document contains at least one reference to terms of said transaction.

24. A medium according to claim 21, wherein said electronic transaction document includes a digital signature of said issuer party participant.

25. A medium according to claim 21, wherein said electronic transaction document includes a digital signature of said non-party participant.

26. A medium according to claim 21, wherein said electronic transaction document includes an encrypted digest covering at least part of said electronic transaction document.

27. A medium according to claim 21, wherein said acceptance note includes a digital signature of said recipient party participant.

28. A medium according to claim 21, wherein said acceptance note includes a digital signature of at least one non-party participant.

29. A medium according to claim 21, wherein said acceptance note includes an encrypted digest covering at least part of said acceptance note.

30. A computer readable storage medium for use with computer apparatus, said medium carrying computer instructions which, when executed by said computer apparatus:

(a) receive an electronic transaction document, said document being non-repudiable by an issuer party participant and describing a transaction between said issuer party participant and at least one recipient party participant, and an indication of verification of said electronic transaction document by a first non-party participant; and

(b) in response to acceptance by said recipient party participant of said transaction as described in said electronic transaction document, provide an acceptance note, non-repudiable by said recipient party participant and evidencing acceptance of said transaction by said recipient party participant.

31. A medium according to claim 30, wherein said electronic transaction document contains terms of said transaction.

32. A medium according to claim 30, wherein said electronic transaction document contains at least one reference to terms of said transaction.

33. A medium according to claim 30, wherein said electronic transaction document includes a digital signature of said issuer party participant.

34. A medium according to claim 30, wherein said electronic transaction document includes a digital signature of said non-party participant.

35. A medium according to claim 30, wherein said electronic transaction document includes an encrypted digest covering at least part of said electronic transaction document.

36. A medium according to claim 30, wherein said acceptance note includes a digital signature of said recipient party participant.

37. A medium according to claim 30, wherein said acceptance note includes a digital signature of at least one non-party participant.

38. A medium according to claim 30, wherein said acceptance note includes an encrypted digest covering at least part of said acceptance note.

39. A computer readable storage medium for use with computer apparatus, said medium carrying computer instructions which, when executed by said computer apparatus:

(a) receive an electronic transaction document, said document being non-repudiable by an issuer party participant and describing a transaction between said issuer party participant and at least one recipient party participant;

(b) verify said electronic transaction document; and

(c) provide said verified electronic transaction document and an indication of said verification to said issuer party participant.

40. A computer readable storage medium for use with computer apparatus, said medium carrying computer instructions which, when executed by said computer apparatus:

(a) receive an electronic transaction document, said document being non-repudiable by an issuer party participant and describing a transaction between said issuer party participant and at least one recipient party participant, said document containing an indication of verification by a non-party participant;

(b) verify said received electronic transaction document; and

(c) provide said verified electronic transaction document to said recipient party participant.

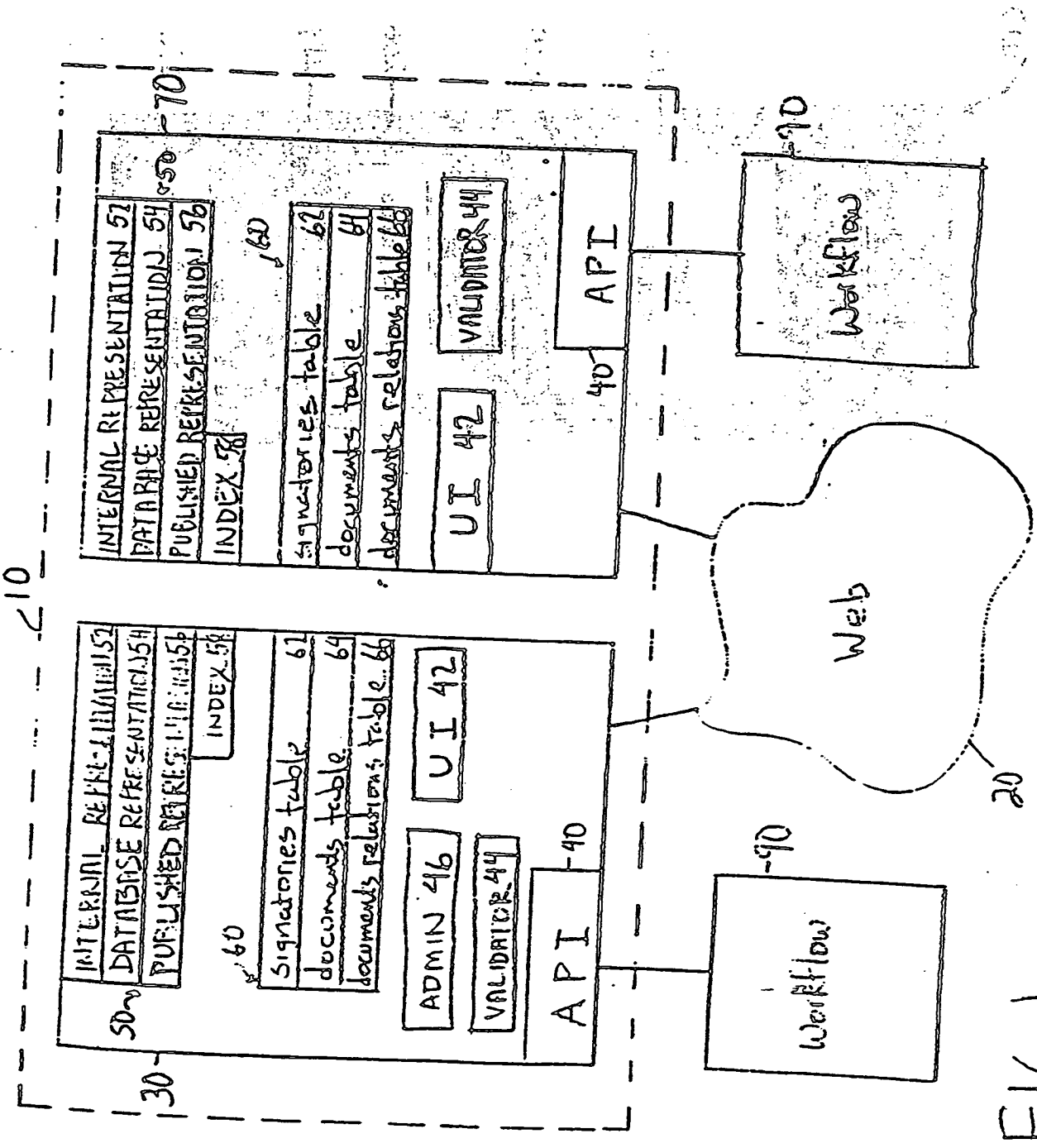


FIG. 1

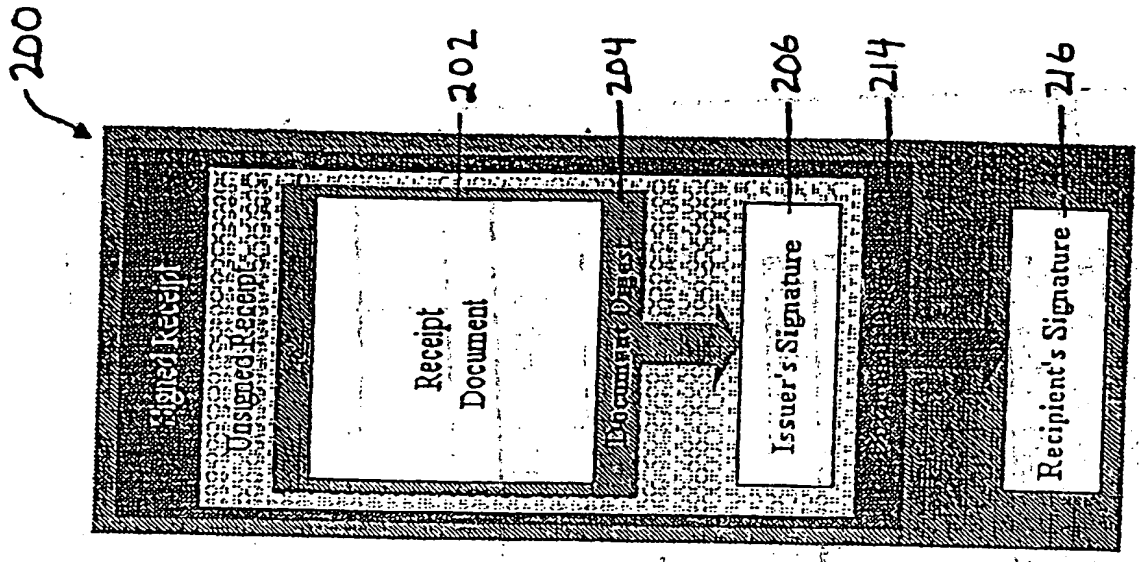

200
202
204
206
214
216
Signed Receipt
Unsigned Receipt
Receipt Document
Document Digest
Issuer's Signature
Recipient's Signature

FIG. 2

FIG. 3

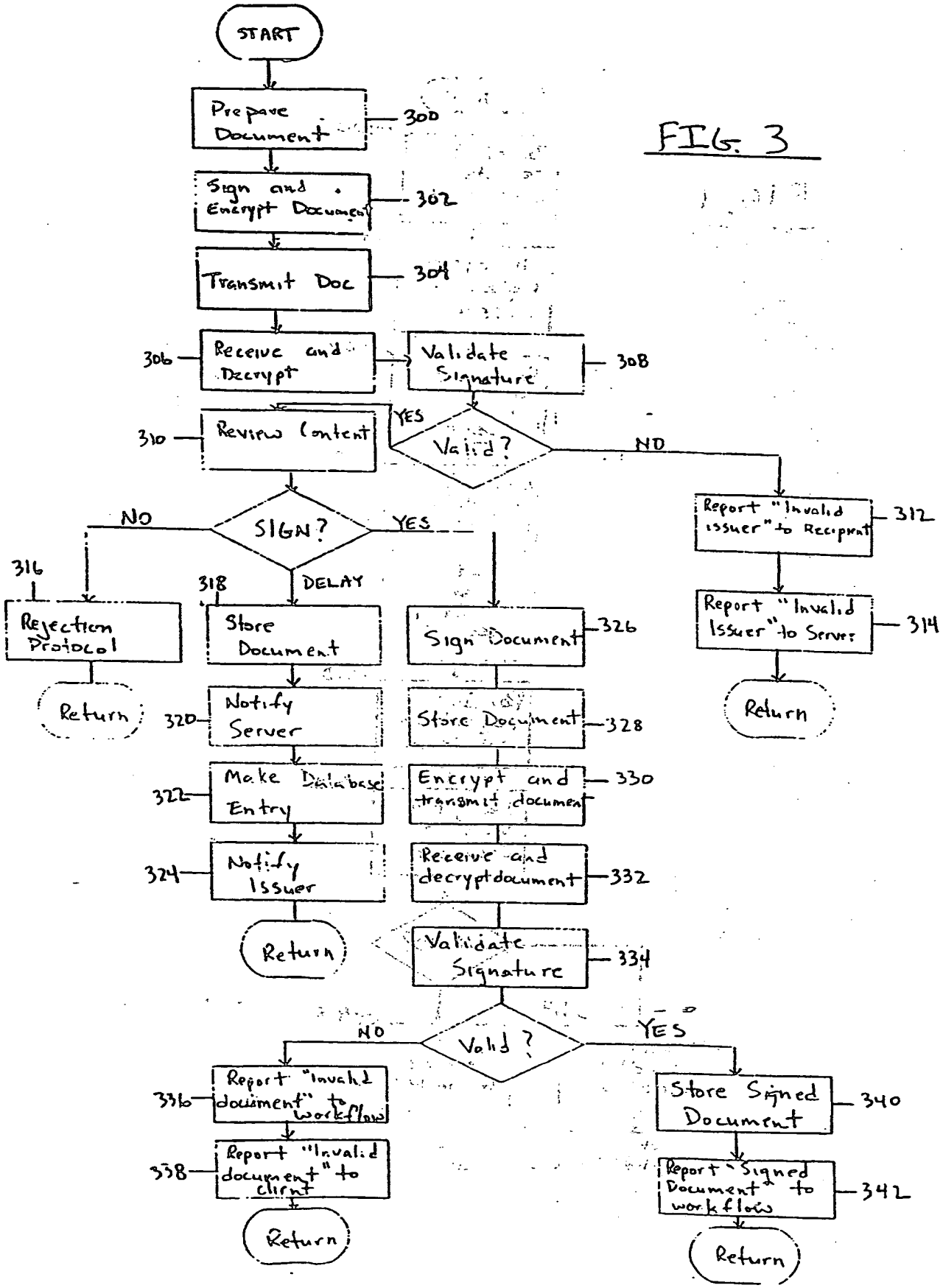


FIG.4

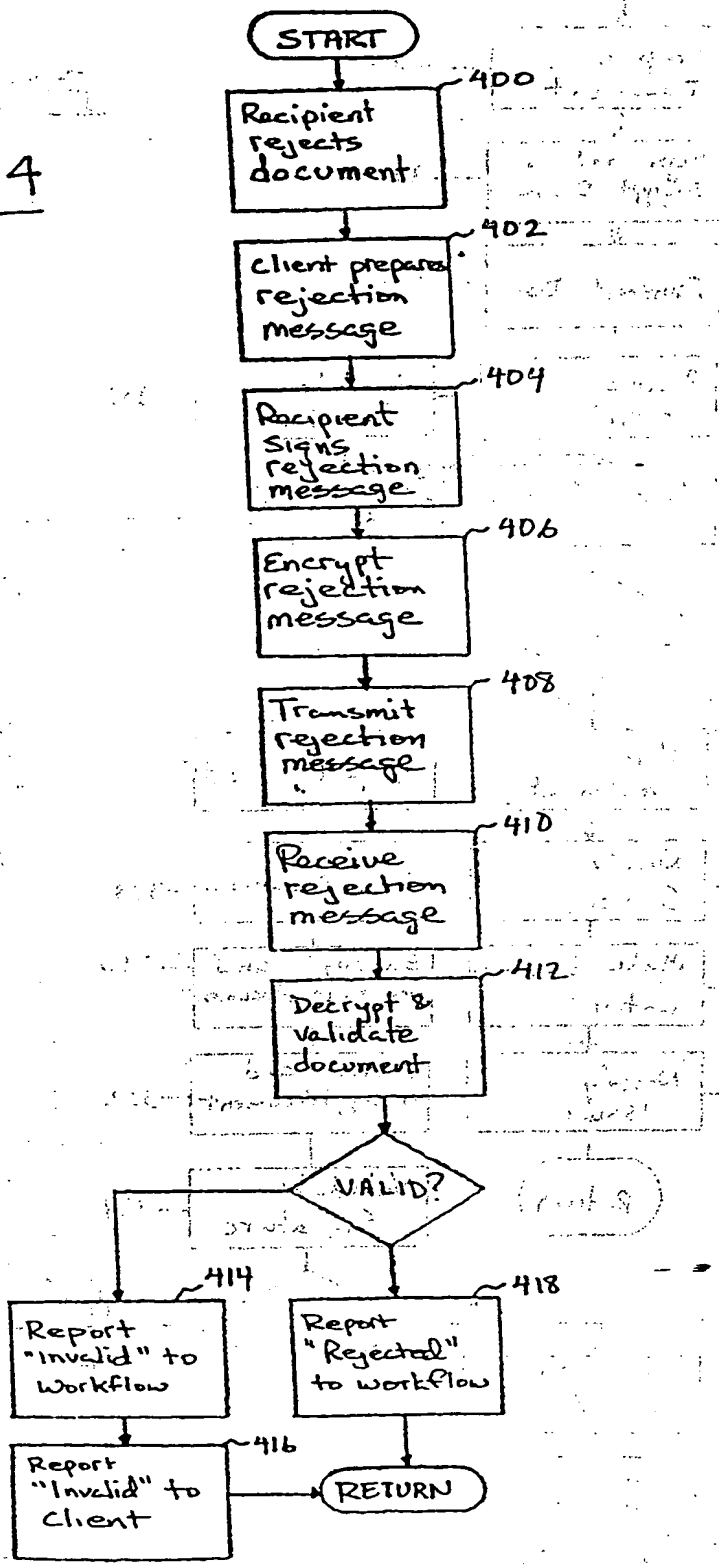


FIG. 5A

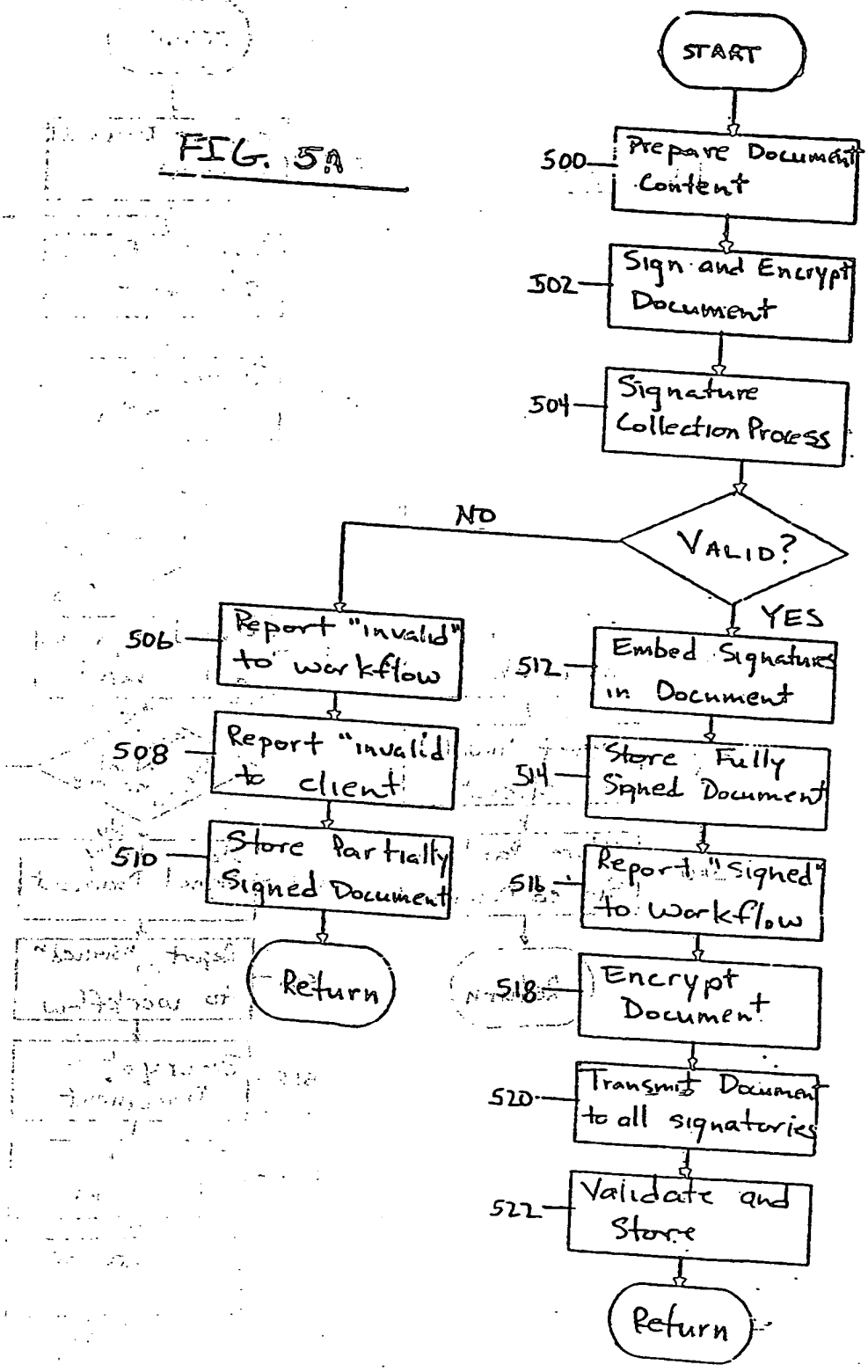
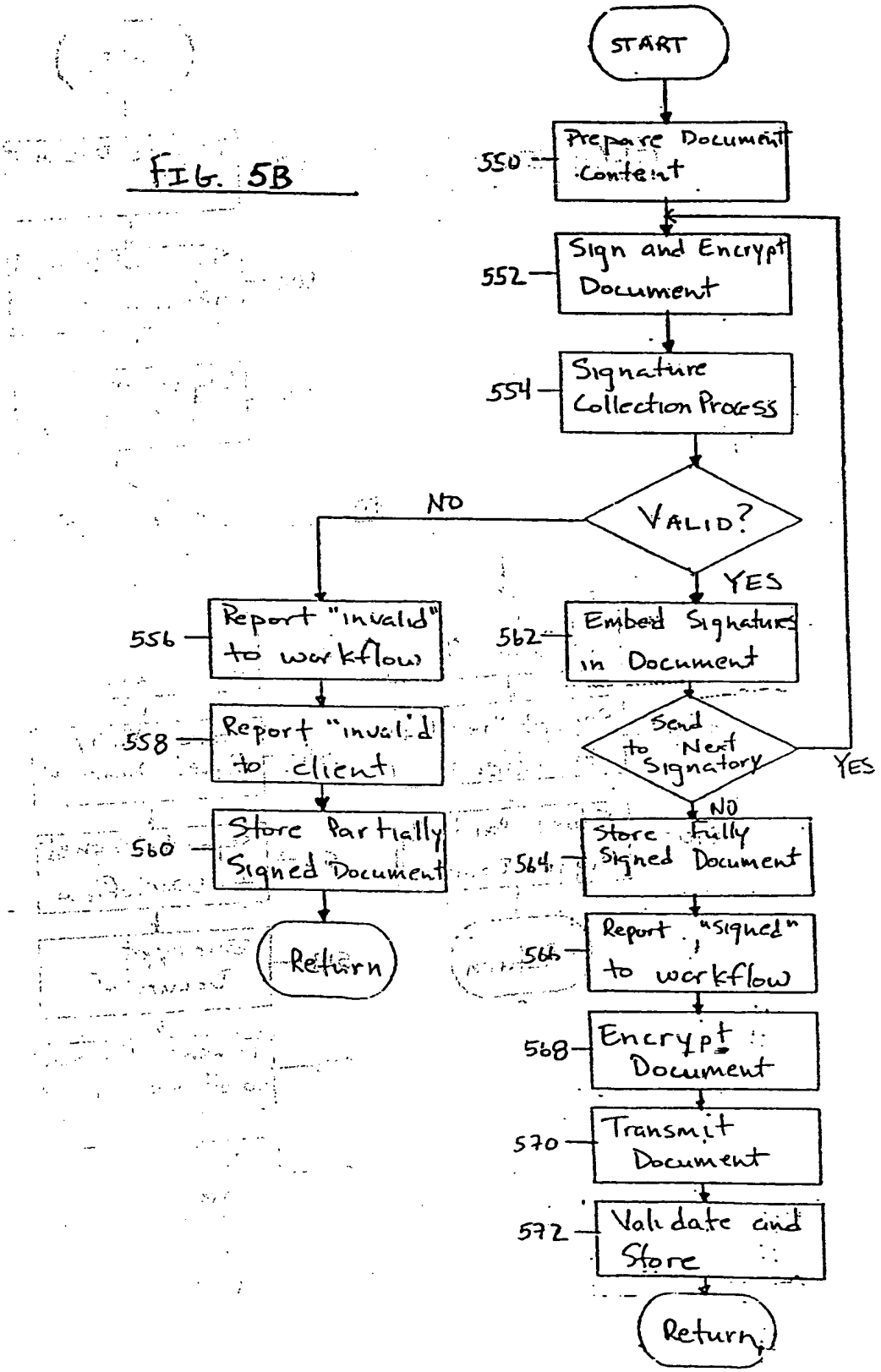


FIG. 5B


START
550
Prepare Document Content
552
Sign and Encrypt Document
554
Signature Collection Process
VALID?
NO
YES
556
Report "invalid" to workflow
558
Report "invalid" to client
560
Store Partially Signed Document
Return
562
Embed Signature in Document
Send to Next Signatory
YES
NO
564
Store Fully Signed Document
566
Report "signed" to workflow
568
Encrypt Document
570
Transmit Document
572
Validate and Store
Return

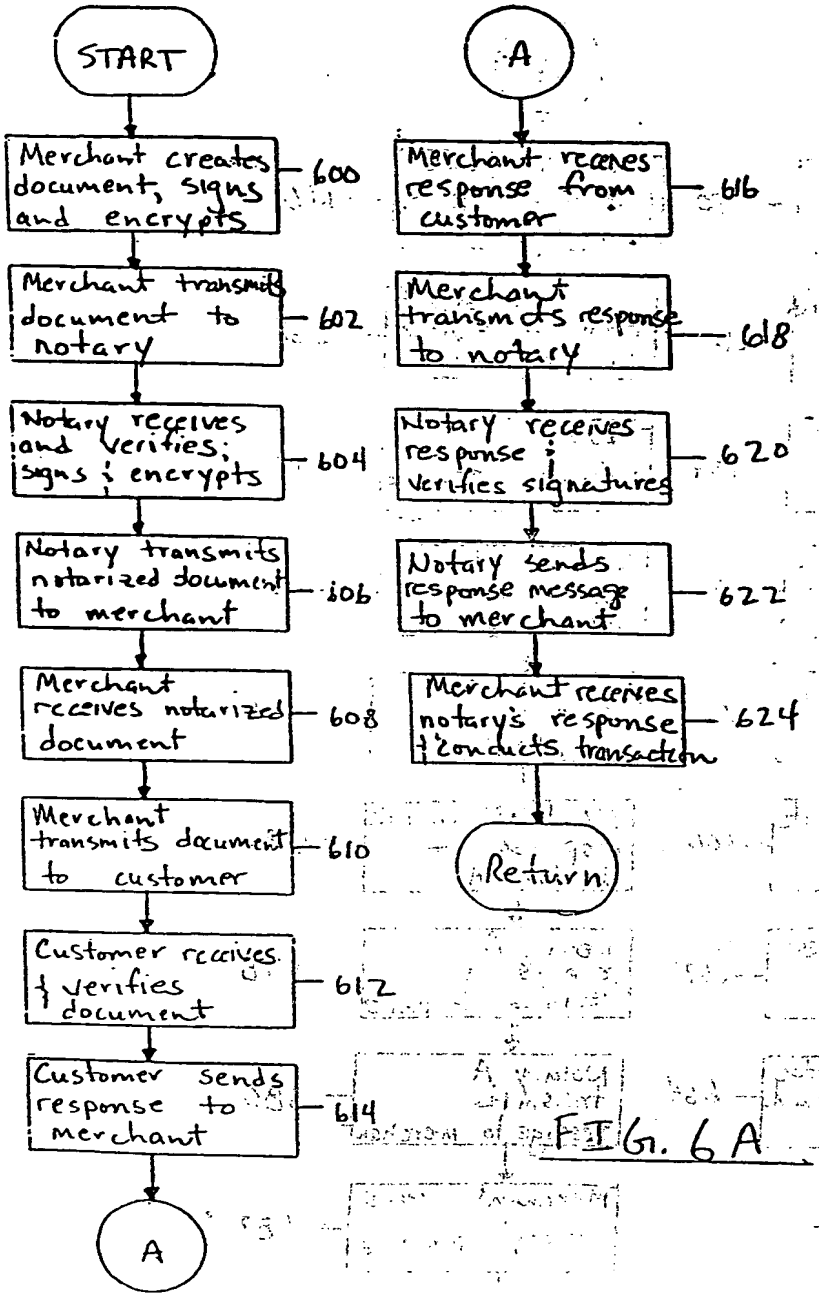


FIG. 6A

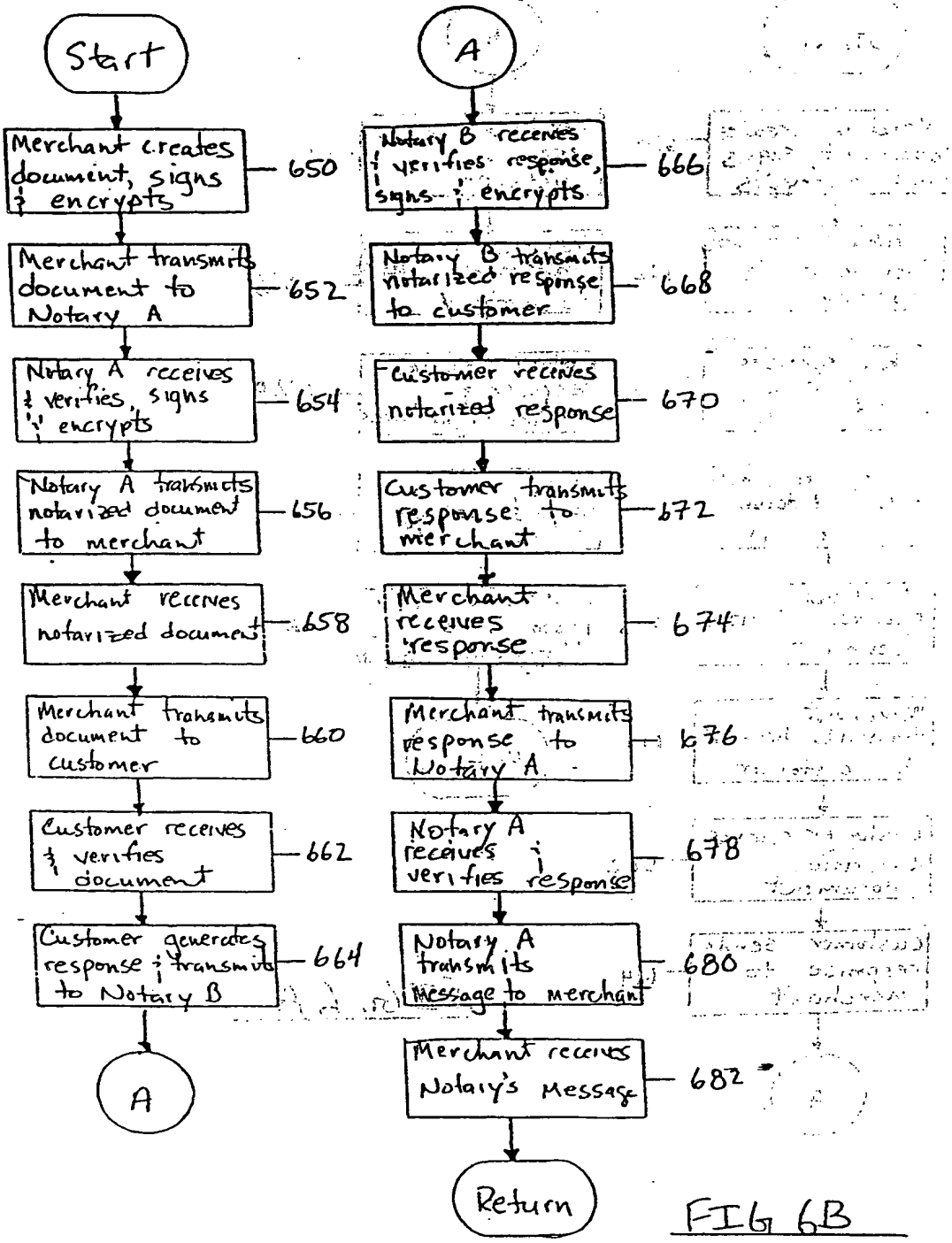

Start
Merchant creates document, signs & encrypts
650
Merchant transmits document to Notary A
652
Notary A receives & verifies, signs & encrypts
654
Notary A transmits notarized document to merchant
656
Merchant receives notarized document
658
Merchant transmits document to customer
660
Customer receives & verifies document
662
Customer generates response & transmits to Notary B
664
A
A
Notary B receives & verifies response, signs & encrypts
666
Notary B transmits notarized response to customer
668
Customer receives notarized response
670
Customer transmits response to merchant
672
Merchant receives response
674
Merchant transmits response to Notary A
676
Notary A receives & verifies response
678
Notary A transmits message to merchant
680
Merchant receives Notary's message
682
Return

FIG 6B

FIG. 7A

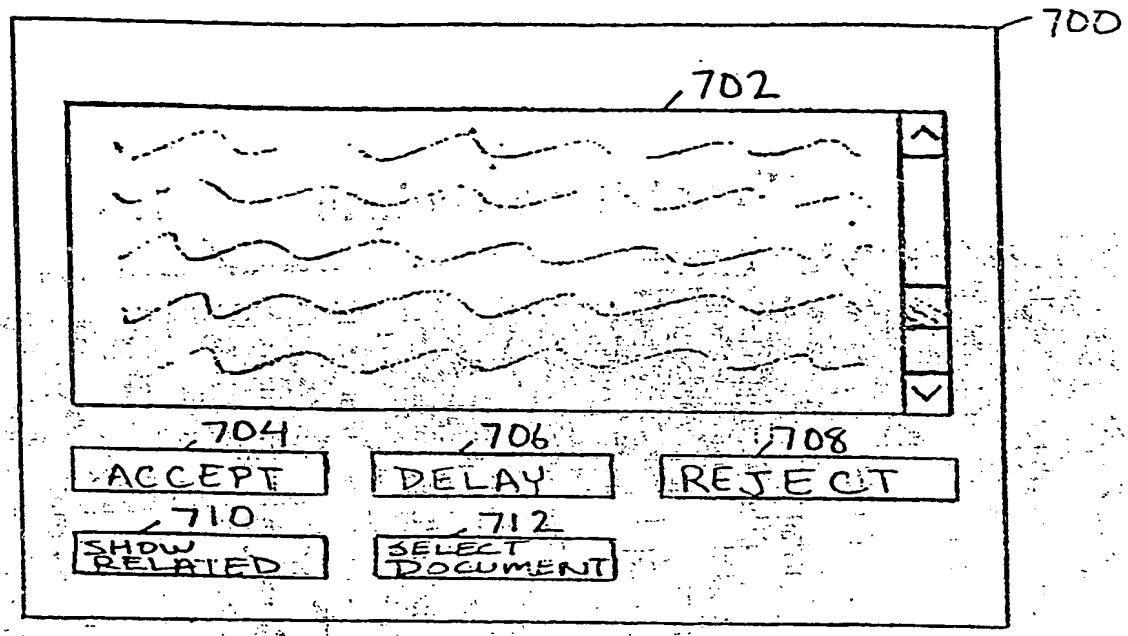
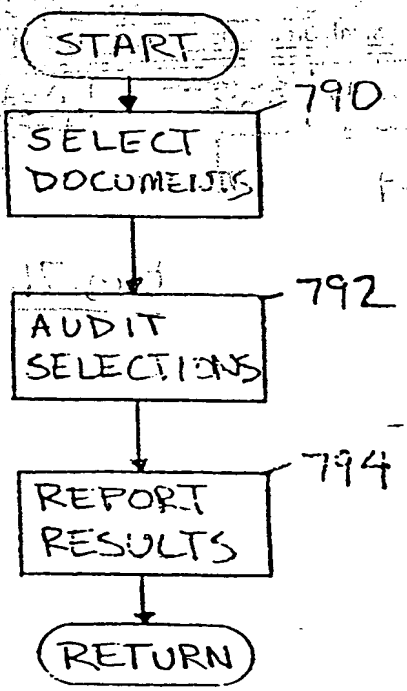


FIG. 7D



Tracking Receipts

720

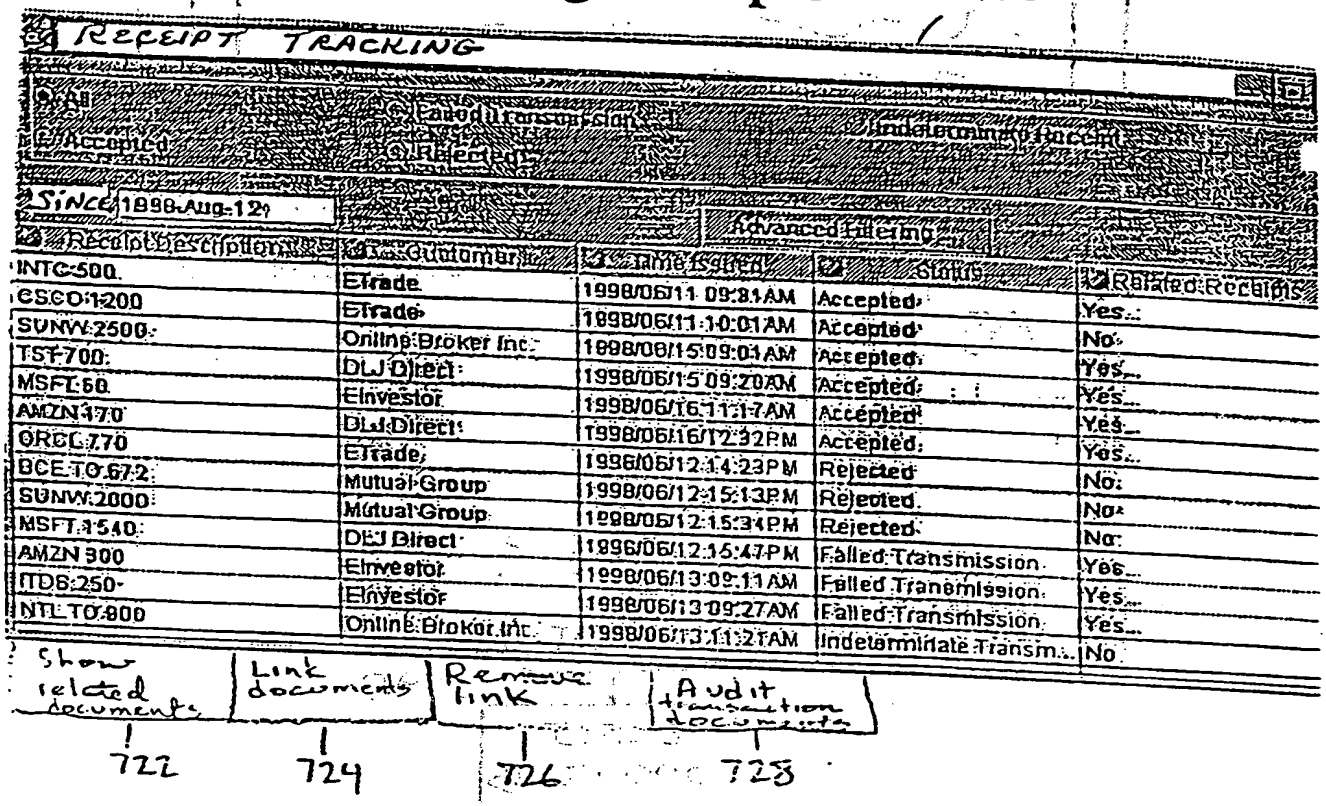


Fig. 7b

List of Related Receipts

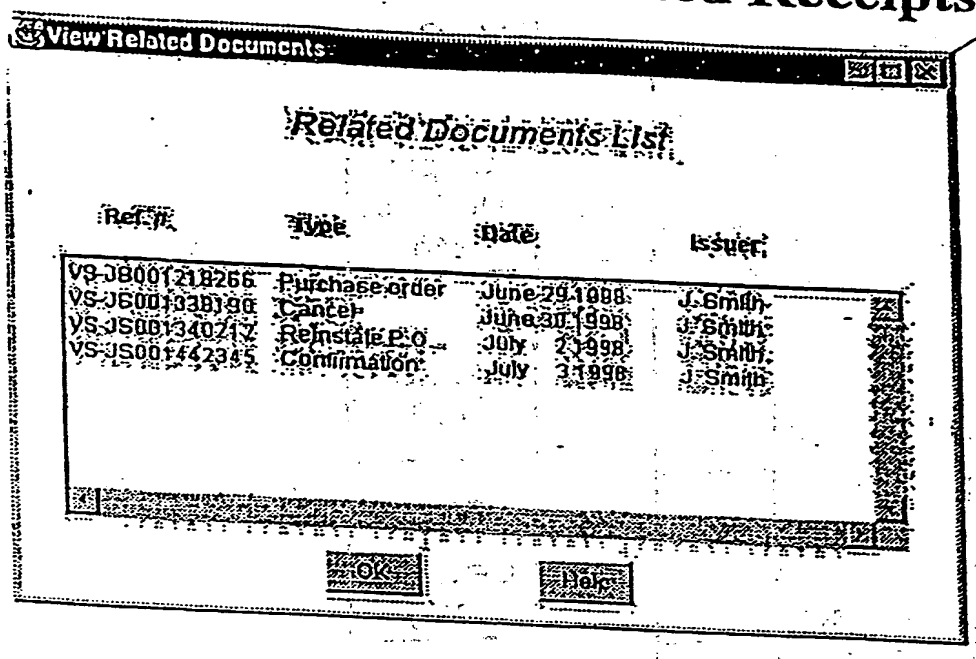


Fig. 7C

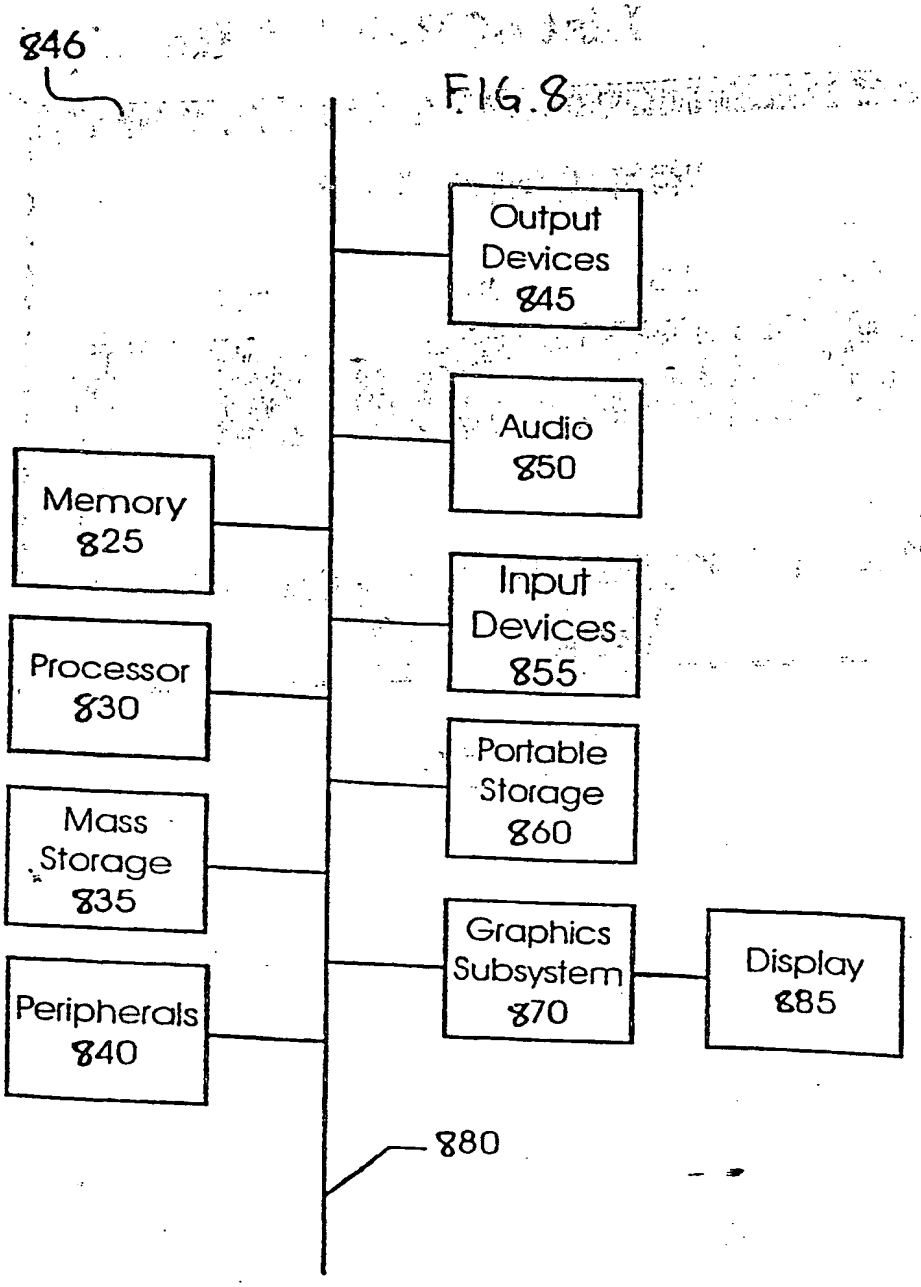


FIG. 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/24570

A. CLASSIFICATION OF SUBJECT MATTER
IPC(6) :G06F 17/60
US CL :380/25
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 380/25

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
235/380, 380/30, 395/200.36, 235/379, 380/4

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
STN

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- A	US 5497422 A [TYSEN et al] 05 March 1996, Abstract, fig 3, item 302, column 1, lines 11-12, column 3, lines 15-17, column 10, lines 4-12, fig 11, item 1110, column 21, lines 35-41, fig 8, item 820, column 2, lines 7-14, 18-26, column 9, lines 21-23, fig 2, item 202, 204, column 22, lines 9-11	1-7, 12-40 --- 8-11

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 DECEMBER 1999	04 FEB 2000
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer JAMES TRAMMEL Telephone No. (703) 305-9768

Form PCT/ISA/210 (second sheet)(July 1992)☆

Best Available Copy